# Indústria de Cartões de Pagamento (PCI)
# Padrão de Segurança de Dados

## Procedimentos de Auditoria de Segurança

## Versão 1.1

Distribuição: Setembro de 2006

# Índice

# Introdução

Os Procedimentos de Auditoria de Segurança da PCI estão projetados para serem usados pelos assessores que executam revisões onsite para os estabelecimentos e prestadores de serviços exigidas para validar a compliance com as exigências do Padrão de Proteção de Dados (DSS) da Indústria de Cartões de Pagamento (PCI). As exigências e os procedimentos de auditoria apresentados neste documento estão baseados no PCI DSS.

Este documento contém o seguinte:

- **Introdução**
- **Informações sobre a Aplicabilidade do PCI DSS**
- **Âmbito da Avaliação da Compliance com as Exigências do PCI DSS**
- **Instruções e Conteúdo para o *Relatório de Compliance* (*Report On Compliance)***
- **Revalidação de Itens em Aberto**
- **Procedimentos da Auditoria de Segurança**

**ANEXOS**

- **Anexo A: Aplicabilidade do PCI DSS para Prestadores de Serviço de Hosting (com Teste de Procedimentos)**
- **Anexo B: Controles de Compensação**
- **Anexo C: Planilha dos Controles de Compensação / Exemplo Preenchido**

# Aplicabilidade das Informações do PCI DSS

A tabela a seguir ilustra os elementos dos dados do portador de cartão e das informações confidenciais da autenticação mais freqüentemente usados; quer a **armazenagem** de cada elemento dos dados seja permitida ou proibida; **e se cada elemento dos dados** deva ser **protegido**. Esta tabela não é completa, mas é apresentada para ilustrar os diferentes tipos de exigências que se aplicam a cada elemento dos dados.

| | Elementos do Dados | Armazenagem Permitida | Proteção Exigida | PCI DSS Exigência 3.4 |
|---|---|---|---|---|
| **Dados do Portador de Cartão** | Número da Conta Primária (PAN) | SIM | SIM* | SIM |
| | Nome do Portador do Cartão* | SIM | SIM* | NÃO |
| | Código do Serviço* | SIM | SIM* | NÃO |
| | Data de Vencimento* | SIM | SIM* | NÃO |
| **Dados Confidenciais de Autenticação**** | Tarja Magnética Completa* | NÃO | NÃO | N/A |
| | CVC2/CVV2/CI | NÃO | NÃO | N/A |
| | PIN / Bloqueador de PIN | NÃO | NÃO | N/A |

* Estes elementos dos dados devem ser protegidos se forem armazenados em conjunto com o PAN. Esta proteção deve ser consistente com as exigências do PCI DSS para a proteção geral do ambiente do portador de cartão. Adicionalmente, outra legislação (por exemplo, relacionada à proteção dos dados pessoais do cliente, privacidade, roubo de identidade ou segurança dos dados) pode exigir uma proteção específica destes dados ou divulgação adequada das práticas da companhia se os dados pessoais relacionados ao cliente estão sendo coletados durante o curso do negócio. O PCI DSS; entretanto, não se aplica se os PANs não forem armazenados, processados ou transmitidos.

** Não armazene dados confidenciais de autenticação subseqüentes à autorização (mesmo se codificados).

# Âmbito da Avaliação da *Compliance* com as Exigências do PCI DSS

Os requisitos de segurança do PCI DSS se aplicam a todos os "componentes do sistema". Um componente do sistema é definido como qualquer componente da rede, servidor ou aplicativo que está incluído ou conectado ao ambiente dos dados do portador do cartão. O ambiente dos dados do portador do cartão é a parte da rede que processa os dados do portador de cartão ou os dados confidenciais de autenticação. Os componentes da rede incluem, mas não se limitam, aos firewalls, switches, routers, pontos de acesso wireless, aplicativos da rede e outros aplicativos de segurança. Os tipos de servidor de rede incluem, mas não se limitam ao seguinte: web, banco de dados, autenticação, correspondência, proxy e network time protocol (NTP) e domain name server (DNS). Os aplicativos incluem todos os adquiridos e customizados, incluindo os aplicativos internos e externos (Internet).

A segmentação adequada da rede que separa os sistemas que armazenam, processam ou transmitem os dados do portador de cartão do restante da rede, pode reduzir o âmbito do ambiente dos dados do portador do cartão. O assessor deve verificar que a segmentação seja adequada para reduzir o âmbito da auditoria.

Um prestador de serviço ou estabelecimento pode usar um provedor externo para administrar os componentes tais como routers, firewalls, bancos de dados, segurança física e/ou servidores. Se assim for, pode haver um impacto na segurança do ambiente dos dados do portador de cartão. Os serviços relevantes do provedor externo devem ser examinados tanto nas 1) auditorias da PCI dos clientes de cada provedor externo; como na 2) auditoria da PCI do provedor externo.

Para os prestadores de serviço, aos quais seja exigido que se submetam a uma revisão anual onsite, a validação da compliance deverá ser executada em todos os componentes do sistema onde os dados do portador de cartão forem armazenados, processados ou transmitidos, a menos que seja especificado de outra forma.

Para os estabelecimentos, aos quais seja exigido que se submetam a uma revisão anual onsite, o âmbito da validação da compliance será concentrado em qualquer sistema ou componente de sistema relacionado com a autorização ou liqüidação onde os dados do portador de cartão forem armazenados, processados ou transmitidos, incluindo o seguinte:

- Todas as conexões externas com a rede do estabelecimento (por exemplo, acesso remoto do funcionário, empresa de cartão de pagamento, acesso por terceiros para processamento e manutenção)
- Todas as conexões de entrada e saída do ambiente de autorização e liquidação (por exemplo, conexões para o acesso pelo funcionário ou para dispositivos tais como firewalls e routers)
- Qualquer dispositivo de armazenagem de dados fora do ambiente de autorização e liquidação onde mais de 500 mil números de contas estejam armazenados. Nota: Mesmo se algum dispositivo de armazenagem de dados ou sistema for excluído da auditoria, o estabelecimento ainda é responsável por assegurar que todos os sistemas que armazenem, processem ou transmitam os dados os dados do portador de cartão estejam de acordo com o PCI DSS
- O ambiente de ponto de venda (POS) é o lugar onde uma transação é aceita no local do estabelecimento (que pode ser uma loja de varejo, restaurante, hotel, posto de gasolina, supermercado ou outro local do POS)

- Se não houver acesso externo ao local do estabelecimento (através da Internet, wireless, virtual private network (VPN), dial-in, broadband ou máquinas publicamente acessíveis, tais como quiosques), o ambiente do POS pode ser excluído

**Wireless**

Se for usada a tecnologia wireless para transmitir, processar ou armazenar os dados dos portadores de cartão (por exemplo, transações de ponto de venda, "line-busting") ou se uma local area network (LAN) estiver conectada em todo ou em parte ao ambiente do portador de cartão (por exemplo, não claramente separado por uma firewall), as Exigências e Procedimentos de Teste para os ambientes wireless devem também ser executados. A segurança do wireless ainda não amadureceu, mas estas exigências especificam que as características básicas de segurança wireless sejam implementadas para oferecer um mínimo de proteção. Visto que as tecnologias wireless ainda não podem ser totalmente seguras, antes que a tecnologia wireless seja instalada, a empresa deve avaliar cuidadosamente a necessidade da tecnologia em comparação ao risco incorrido. Considere a instalação apenas para a transmissão de dados não confidenciais ou espere para que a tecnologia se torne mais segura.

**Prestador de Serviço Externo**

Para as entidades que contratam um prestador de serviço externo para fazer o processamento, transmissão ou armazenagem dos dados dos portadores de cartão, o *Relatório de Compliance* deve documentar o papel desempenhado por cada prestador de serviço. Além disso, os prestadores de serviço são responsáveis pela validação da sua própria compliance em relação às exigências do PCI DSS, independentemente da auditoria dos seus clientes. Adicionalmente, os estabelecimentos e prestadores de serviço devem exigir contratualmente que todos os prestadores de serviço externos associados com acesso aos dados dos portadores de cartão cumpram com o PCI DSS. *Consulte a Exigência 12.8 neste documento para obter maiores detalhes*.

**Amostragem**

O assessor pode selecionar uma amostra representativa dos componentes do sistema para teste. A amostra deve ser uma seleção representativa de todos os tipos de componentes do sistema e incluem uma variedade de sistemas operacionais, funções e aplicativos que sejam relevantes para a área a ser revisada. Por exemplo, o revisor pode escolher os servidores Sun rodando Apache WWW, servidores NT rodando Oracle, sistemas de mainframe rodando aplicativos legacy de processamento de cartão, servidores de transferência de dado rodando HP-UX, Servidores Linux rodando MYSQL. Se todos os aplicativos rodarem sob um único OS (por exemplo, NT, Sun), então a amostra deve incluir uma variedade de aplicativos (por exemplo, servidores de banco de dados, servidores web, servidores de transferência de dados).

*Ao selecionar amostras das lojas dos estabelecimentos ou para estabelecimentos de franquias, os assessores devem considerar o seguinte:*

- Se houver processos padrões exigidos pelo PCI DSS em funcionamento para cada loja seguir, a amostra pode ser menor que o necessário se comparado com o caso de não haver processos padrões para proporcionar a garantia razoável de que cada loja está configurada de acordo com o processo padrão.

- Se houver mais de um tipo de processo padrão em funcionamento (por exemplo, para diferentes tipos de lojas), então a amostra deve ter um tamanho suficiente para incluir as lojas seguradas com cada tipo de processo.
- Se não houver processos padrões do PCI DSS em funcionamento e cada loja for responsável por seus próprios processos, então o tamanho da amostra deve ser maior para assegurar que cada loja compreenda e implemente apropriadamente as exigências do PCI DSS.

**Controles de Compensação**

Os controles de compensação devem ser documentados pelo assessor e incluídos com a submissão do Relatório de Compliance, como mostrado no Anexo C – Planilha dos Controles de Compensação / Exemplo Preenchido.

Consultar o Glossário do PCI DSS, Abreviação e Acrônimos para as definições de “controles de compensação”.

# Instruções e Conteúdo para o Relatório de Compliance

Este documento deve ser usado pelos assessores como um modelo para criar o *Relatório de Compliance*. A entidade auditada deve atender a cada uma das exigências de relatório das respectivas empresas de cartão de pagamento para garantir que cada uma reconheça o status de compliance da entidade. Favor contatar cada empresa de cartão de pagamento para determinar as exigências e instruções para relatórios de cada companhia. Todos os assessores devem seguir as instruções para o conteúdo e formato do relatório ao completar um *Relatório de Compliance*:

**1. Informação de Contato e Data do Relatório**

- Inclui a informação de contato para o estabelecimento ou prestador de serviço e assessor
- Data do relatório

**2. Resumo Executivo**

Inclui o seguinte:

- Descrição do negócio
- Lista dos prestadores de serviço e outras entidades com as quais a empresa compartilha os dados dos portadores de cartão
- Lista do relacionamento com processadores
- Descrever se a entidade está diretamente conectada à empresa de cartão de pagamento
- Para os estabelecimentos, os produtos de POS usados
- Qualquer entidade em que a empresa possua total controle acionário e que exija compliance com o PCI DSS
- Qualquer entidade internacional que exija compliance com o PCI DSS
- Qualquer LAN wireless e/ou Terminais de POS wireless conectados ao ambiente do portador de cartão

### 3. Descrição do Âmbito do Trabalho e Abordagem a ser Tomada

- Versão dos documentos dos Procedimentos da Auditoria de Segurança usados para conduzir o levantamento
- Prazo do levantamento
- Ambiente no qual o levantamento se focaliza (por exemplo, pontos de acesso à Internet pelo cliente, rede corporativa interna, pontos de processamento para a empresa de cartão de pagamento)
- Qualquer área excluída da revisão
- Breve descrição ou esquema de alto nível da topologia da rede e controles
- Lista dos indivíduos entrevistados
- Lista dos documentos revisados
- Lista de hardware e software críticos (por exemplo, banco de dados e codificação) em uso
- Para as revisões do Managed Service Provider (MSP), delinear claramente quais são as exigências deste documento que devem ser aplicadas ao MSP (e se encontram incluídas na revisão), e quais não se encontram incluídas na revisão e são responsabilidade dos clientes do MSP incluir em suas próprias revisões. Adicionar a informação sobre qual dos endereços de IP do MSP são scanned como parte dos scans trimestrais de vulnerabilidade do MSP e quais endereços de IP são de responsabilidade dos clientes do MSP incluir em seus próprios scans trimestrais

### 4. Resultados dos Scans Trimestrais

- Resumir os resultados dos quatro scans trimestrais mais recentes nos comentários da Exigência 11.2
- O scan deve cobrir todos os endereços de IP acessíveis externamente (Internet-facing) existentes na entidade

### 5. Conclusões e Observações

- Todos os assessores devem utilizar o modelo a seguir para prover um relatório com descrições detalhadas e conclusões sobre cada exigência e sub-exigência
- Onde for aplicável, documentar qualquer controle compensatório considerado para concluir que um controle está instalado
- Consultar o Glossário do PCI DSS, Abreviação e Acrônimos para as definições de “controles de compensação”.

## Revalidação de Itens em Aberto

É exigido um relatório dos “controles instalados” (controls in place) para verificar o compliance. Se um relatório inicial pelo auditor/assessor contiver “itens em aberto”, o estabelecimento/prestador de serviço deve corrigir estes itens antes da validação ser completada. O assessor/auditor então deve reavaliar se a correção foi feita e atendeu a todas as exigências. Após a reavaliação, o assessor deve emitir um novo *Relatório de Compliance*, verificando que o sistema está totalmente em compliance e submetê-lo de acordo com as instruções. (Ver acima).

# Construa e Mantenha uma Rede Segura

## Exigência 1: Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão

Firewalls são dispositivos no computador que controlam o tráfego de entrada e de saída admitido na rede da empresa via computador, bem como o tráfego nas áreas mais críticas dentro da rede interna da empresa. Um firewall examina todo o tráfego da rede e bloqueia as transmissões que não atendam a critérios específicos de segurança.

Todos os sistemas devem estar protegidos contra o acesso não autorizado via Internet, seja entrando no sistema como e-commerce, acesso à Internet pelo funcionário através de browsers ou e-mail. Geralmente, o acesso considerado insignificante como o de entrada ou de saída da Internet pode oferecer uma conexão desprotegida para sistemas importantes. Os firewalls são o principal mecanismo de proteção para qualquer rede de computadores.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **1.1** Estabeleça um padrão de configuração de firewall que inclua o seguinte: | **1.1** Obtenha e inspecione os padrões da configuração do firewall e outras documentações especificadas abaixo para obter evidência de que os padrões estão completos. Preencha cada item nesta seção | | | |
| **1.1.1** Um processo formal de aprovação e teste de todas as conexões externas e mudanças na configuração do firewall | **1.1.1** Verifique se os padrões da configuração do firewall incluem um processo formal para todas as mudanças no mesmo, incluindo testes e a aprovação da administração para todas as mudanças nas conexões externas da rede e na configuração do firewall | | | |
| **1.1.2** Um diagrama atualizado da rede com todas as conexões que levem aos dados do portador de cartão, incluindo qualquer rede wireless | **1.1.2.a** Verifique se existe um diagrama atualizado da rede e que o mesmo documenta todas as conexões para os dados dos portadores de cartão, incluindo quaisquer redes | | | |
| | **1.1.2.b**. Verifique se o diagrama é mantido atualizado | | | |
| **1.1.3** Exigências para um firewall em cada conexão com a Internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna | **1.1.3** Verifique se os padrões de configuração do firewall incluem as exigências de um firewall em cada uma das conexões de Internet e entre qualquer DMZ e a Intranet. Verifique se os diagramas atualizados da rede são consistentes com os padrões de configuração do firewall | | | |
| **1.1.4** Descrição dos grupos, tarefas e responsabilidades para a administração lógica dos | **1.1.4** Verifique se os padrões da configuração do firewall incluem a descrição dos grupos, finalidade e responsabilidades para a administração lógica dos | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| componentes da rede | componentes da rede | | | |
| **1.1.5** Lista documentada dos serviços e ports necessários para o negócio | **1.1.5** Verifique se os padrões da configuração do firewall incluem uma lista documentando os serviços/ports necessários para o negócio | | | |
| **1.1.6** Justificação e documentação de qualquer protocolo disponível além do hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH) e virtual private network (VPN) | **1.1.6** Verifique se os padrões da configuração do firewall incluem uma justificativa e documentação para quaisquer protocolos disponíveis além do HTTP, SSL, SSH e VPN | | | |
| **1.1.7** Justificativa e documentação de quaisquer protocolos de riscos permitidos (por exemplo, file transfer protocol (FTP), que inclua a razão para o uso do protocolo e características de segurança implementada**)** | **1.1.7.a** Verifique se os padrões da configuração do firewall incluem uma justificativa e documentação para quaisquer protocolos de riscos permitidos (por exemplo, FTP), que inclua a razão para o uso do protocolo e características de segurança implementadas | | | |
| | **1.1.7.b** Examine a documentação e configurações para cada serviço em uso para obter evidência de que o serviço é necessário e seguro | | | |
| **1.1.8** Revisão trimestral dos conjuntos de regras para o firewall e router | **1.1.8.a** Verifique se os padrões de configuração do firewall exigem uma revisão trimestral do conjunto de regras do firewall e router | | | |
| | **1.1.8.b** Verifique se o conjunto de regras é revisado a cada trimestre | | | |
| **1.1.9** Padrões de configuração para os routers | **1.1.9** Verifique se os padrões de configuração do firewall existem tanto para os firewalls como para os routers | | | |
| **1.2** Construa uma configuração de firewall que não permita qualquer tráfego advindo das redes e hosts, “não confiáveis”, com exceção dos protocolos necessários ao ambiente de dados do portador de cartão. | **1.2** Escolha uma amostra dos firewalls/routers. 1) entre a Internet e a DMZ e 2) entre a DMZ e as redes internas. A amostra deve incluir o choke router na Internet, o router da DMZ e firewall, a DMZ do segmento do portador de cartão, o perimeter router e o segmento interno da rede do portador de cartão. Examine as configurações do firewall e router para verificar se o tráfego de entrada e saída encontra-se limitado apenas aos protocolos que sejam necessários ao ambiente dos dados do portador de cartão | | | |
| **1.3** Construa uma configuração de firewall que restrinja as | **1.3** Examine as configurações do firewall/router para verificar se as conexões estão restritas entre os servidores de | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| conexões entre os servidores de acesso público e qualquer componente do sistema que armazene os dados do portador de cartão, incluindo quaisquer conexões de redes wireless. Esta configuração de firewall deve incluir: | acesso público e os componentes de armazenagem de dados dos portadores de cartão, como a seguir: | | | |
| **1.3.1** Restrição ao tráfego de entrada da Internet aos endereços do internet protocol (IP) dentro da DMZ (filtros de ingresso) | **1.3.1** Verifique se o tráfego de entrada da Internet encontra-se limitado aos endereços do IP dentro da DMZ | | | |
| **1.3.2** Não permita que os endereços internos passem da Internet para a DMZ | **1.3.2** Verifique se os endereços internos não podem migrar da Internet para a DMZ | | | |
| **1.3.3** Implementação *stateful*, também conhecida como dynamic packet filtering (ou seja, apenas as conexões ”instaladas” são permitidas na rede) | **1.3.3** Verifique se o firewall executa uma inspeção stateful (dynamic packet filtering). [Apenas as conexões instaladas devem ser permitidas e apenas se elas estiverem associadas com uma sessão estabelecida previamente (rode NMAP em todos os ports TCP e UDP com “syn reset” ou ”syn ack” bits ajustado – uma resposta significa que os packets são admitidos mesmo que eles não sejam parte de uma sessão previamente estabelecida)] | | | |
| **1.3.4** Colocação do banco de dados em uma zona interna da rede, separada da DMZ | **1.3.4** Verifique se o banco de dados se encontra em uma zona interna da rede, separado da DMZ | | | |
| **1.3.5** Restrição do tráfego de saída apenas para o que for necessário ao ambiente de dados do portador de cartão | **1.3.5** Verifique se o tráfego de entrada e de saída se encontra limitado ao estritamente necessário e documentado para o ambiente do portador de cartão e que as restrições estejam documentadas | | | |
| **1.3.6** Arquivos de configuração de router seguros e sincronizados. Por exemplo, arquivos de configuração de execução (usados para o funcionamento normal dos routers) e arquivos de configuração de partida (usados | **1.3.6** Verificar se os arquivos de configuração do router se encontram seguros e sincronizados [por exemplo: se os arquivos de configuração executados (usados para a execução dos routers) e arquivos de configuração de inicialização (usados quando as máquinas são religadas) possuem as mesmas configurações de segurança] | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| quando as máquinas são religadas) devem possuir a mesma configuração segura | | | | |
| **1.3.7** Bloqueio de qualquer outro tráfego de entrada e saída que não seja especificamente permitido | **1.3.7** Verifique se todos os outros tráfegos de entrada e saída não cobertos no item 1.2 e 1.3 acima estejam especificamente bloqueados | | | |
| **1.3.8** Instalação de um perímetro de firewalls entre quaisquer redes wireless e o ambiente dos dados dos portadores de cartões e a configuração destes firewalls para bloquear qualquer tráfego do ambiente wireless ou controlar qualquer tráfego (se tal tráfego for necessário para o objetivo do negócio) | **1.3.8** Verifique se existem firewalls de perímetro instalados entre quaisquer redes wireless e sistemas que armazenem os dados dos portadores de cartão e se estes firewalls bloqueiam ou controlam (se tais tráfegos são necessários para o objetivo do negócio) qualquer tráfego do ambiente wireless para os sistemas que armazenam os dados dos portadores de cartão | | | |
| **1.3.9** Instalação de um software de firewall individual em qualquer dispositivo portátil e computadores de propriedade do funcionário que possua conexão direta com a Internet (por exemplo, laptops usados pelos funcionários), os quais sejam usados para o acesso à rede da organização | **1.3.9** Verifique se os dispositivos portáteis e/ou computadores de propriedade do funcionário com conexão direta à Internet (por exemplo, laptops usados pelos funcionários) e que são usados para o acesso à rede da organização, possuem um software de firewall pessoal instalado e ativado, o qual é configurado pela organização dentro de padrões específicos e não alteráveis pelo funcionário | | | |
| **1.4** Proíba o acesso público direto entre as redes externas e qualquer componente do sistema que armazene os dados do portador de cartão (por exemplo, banco de dados, registros, trace files) | **1.4** Para determinar se o acesso direto entre as redes externas públicas e os componentes do sistema que armazenam os dados dos portadores de cartão está proibido, execute o seguinte, *especificamente* para a implementação da configuração do firewall/router entre a DMZ e a redes interna: | | | |
| **1.4.1** Implementação de uma DMZ para filtrar e verificar todo o tráfego e para bloquear qualquer rota direta para a entrada e saída | **1.4.1** Examine as configurações do firewall/router e verifique se não existe qualquer rota direta de entrada e saída para o tráfego da Internet | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| do tráfego da Internet | | | | |
| **1.4.2** Restrição do tráfego de saída dos aplicativos de cartões de pagamento para os endereços do IP dentro da DMZ | **1.4.2** Examine as configurações do firewall/router e verifique se o tráfego interno de saída dos aplicativos do portador de cartão podem ter acesso apenas aos endereços de IP dentro da DMZ | | | |
| **1.5** Implemente a ocultação do Internet Protocol (IP) para impedir que os endereços internos sejam traduzidos e revelados na Internet. Use tecnologias que implementem o espaço de endereço RFC 1918, tais como port address translation (PAT) ou network address translation (NAT). | **1.5** Para uma amostra dos componentes de firewall/router acima, verificar que a NAT ou outra tecnologia usando o espaço de endereço RFC 1918 seja usada para restringir a transmissão dos endereços de IP da rede interna para a Internet (disfarce do IP) | | | |

## Exigência 2: Não use as senhas padrão de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços.

Hackers (externos e internos à empresa) geralmente usam as senhas padrão dos prestadores de serviços e outros parâmetros padrão para comprometer os sistemas. Estas senhas e parâmetros são bastante conhecidos nas comunidades de hackers e facilmente obtidos através de informações públicas.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **2.1** Mude sempre os padrões estabelecidos pelo prestador de serviço **antes** da instalação de um sistema na rede (por exemplo, senhas, simple network management protocol (SNMP) community strings e eliminação de contas desnecessárias). | **2.1** Escolha uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, e tente se conectar (com a ajuda do administrador do sistema) aos dispositivos usando as contas e senhas padrão fornecidas pelo fornecedor/prestador de serviço, para verificar se as mesmas foram mudadas. (Use os manuais dos fornecedores e fontes na Internet para encontrar as contas e senhas dos fornecedores/prestadores de serviço) | | | |
| **2.1.1 Nos ambientes wireless**, mudar os padrões de wireless do prestador de serviço, incluindo, mas não limitado a, chaves de wireless equivalent privacy (WEP), padrão do service set identifier (SSID), senhas e SNMP community strings. Desativar a transmissão de SSID. Ativar o Wi-Fi protected access (WPA e WPA2) para a codificação e autenticação quando for capacitado a operar o WPA. | **2.1.1** Verifique o seguinte com relação aos parâmetros padrões do fornecedor para os ambientes wireless:<br>• Que as chaves WEP foram mudadas do padrão no momento da instalação e são mudadas a qualquer momento sempre que alguém com conhecimento das chaves deixa a empresa ou muda de função<br>• Que o SSID padrão foi modificado<br>• Que a transmissão do SSID foi desativada<br>• Que os padrões SNMP community strings nos pontos de acesso foram mudados<br>• Que as senhas padrão nos pontos de acesso foram mudadas<br>• Que a tecnologia WPA ou WPA2 foi ativada se o sistema wireless suportar WPA<br>• Outros padrões de segurança de fornecedores de wireless, se forem aplicáveis | | | |
| **2.2** Desenvolva padrões de configuração para todos os componentes do sistema. Certifique-se de que estes padrões atendam a todas as vulnerabilidades e que sejam consistentes com os padrões do sistema aceito pela indústria como definido, por exemplo, pela | **2.2.a** Examine os padrões de configuração do sistema da organização para os componentes de redes, servidores críticos e pontos de acesso wireless, e verifique se os padrões de configuração do sistema são consistentes com os padrões do sistema aceito pela indústria como definido, por exemplo, pela SANS, NIST e CIS | | | |
| | **2.2.b** Verifique se os padrões de configuração do sistema incluem cada item abaixo (2.2.1 a 2.2.4) | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), e Center for Internet Security (CIS). | **2.2.c** Verifique se os padrões de configuração do sistema são aplicados quando os novos sistemas são configurados | | | |
| **2.2.1** Implemente apenas uma função principal por servidor (*por exemplo, servidores da web, servidores de banco de dados e DNS devem ser implementados em servidores separados*) | **2.2.1** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, verifique se há apenas uma função primária implementada por servidor | | | |
| **2.2.2** Desative todos os serviços e protocolos sem segurança e desnecessários (serviços e protocolos não diretamente necessários para executar a função específica do dispositivo) | **2.2.2** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, inspecione os serviços ativos do sistema, daemons e protocolos. Verifique se os serviços ou protocolos desnecessários ou sem segurança não se encontram ativados ou se estão justificados e documentados como para um uso apropriado do serviço (por exemplo, o FTP não é usado ou é codificado via SSH ou outra tecnologia) | | | |
| **2.2.3** Configure os parâmetros de segurança do sistema para prevenir o uso incorreto | **2.2.3.a** Entreviste os administradores do sistema e/ou gerentes de segurança para verificar se eles possuem o conhecimento das configurações dos parâmetros de segurança comuns dos seus sistemas operacionais, servidores de banco de dados, servidores da web e sistemas wireless | | | |
| | **2.2.3.b** Verifique se os parâmetros comuns de segurança estão incluídos nos padrões de configuração do sistema | | | |
| | **2.2.3.c** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, verifique se os parâmetros comuns de segurança estão configurados apropriadamente | | | |
| **2.2.4** Remova todas as funcionalidades desnecessárias, tais como scripts, drivers, características, sub-sistemas, sistemas de arquivo e servidores de web | **2.2.4** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, verifique se todas as funções desnecessárias (por exemplo, scripts, drivers, características, sub-sistemas, sistemas de arquivo, etc.) foram removidas. Também verifique se as funções habilitadas estão documentadas, suportam uma configuração de segurança e | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| desnecessários | que apenas funcionalidades documentadas estão presentes nas máquinas da amostra | | | |
| **2.3** Codifique todo o acesso administrativo que não seja via teclado. Use tecnologias tais como SSH, VPN, ou SSL/TLS (transport layer security) para a administração baseada na web e outro acesso administrativo via unidade de teclado | **2.3** Da amostra dos componentes do sistema, servidores críticos e pontos de acesso, verifique se um acesso administrativo que não seja via teclado esteja codificado, por intermédio da:<br>• Observação de um log de administrador em cada sistema para determinar se a SSH (ou outro método de codificação) é invocada antes que a senha do administrador seja solicitada<br>• Revisão dos arquivos de serviço e parâmetros nos sistemas para determinar se Telnet ou outros comandos remotos de login não se encontram disponíveis para o uso interno<br>• Verificação de que o acesso do administrador à interface de administração wireless esteja codificado com SSL/TLS. Alternativamente, verificar se os administradores não podem se conectar remotamente à interface de administração wireless (toda a administração dos ambientes wireless é feita apenas através do console) | | | |
| **2.4** Prestadores de serviço de hosting devem proteger o ambiente e os dados de cada entidade à qual prestam o serviço. Estes provedores devem atender a exigências específicas de acordo com o especificado no Anexo A: "Aplicabilidade do PCI DSS para Prestadores de Serviço de Hosting" | **2.4** Executar os procedimentos de teste de **A.1.1** a **A.1.4** especificados no Anexo A, "Aplicabilidade do PCI DSS para Prestadores de Serviço de Hosting (com Procedimentos de Teste)" para as auditorias da PCI dos **Prestadores Compartilhados de Serviço de Hosting**, para verificar se os mesmos protegem o ambiente e os dados das entidades (estabelecimentos e provedores) às quais prestam o seu serviço | | | |

# Proteja os Dados do Portador de Cartão

## Exigência 3: Proteja os dados armazenados do portador de cartão

A codificação é um componente crítico para a proteção dos dados do portador de cartão. Se um intruso burla os controles de segurança da rede e obtém acesso ao dado codificado sem as chaves de codificação adequadas, os dados são ilegíveis e inúteis para o indivíduo. Outros métodos efetivos de proteção para os dados armazenados deveriam ser considerados como oportunidades de diminuir o risco potencial. Por exemplo, os métodos para minimização do risco incluem não armazenar os dados do portador de cartão a menos que absolutamente necessário, truncar os dados do portador de cartão se o PAN completo não for necessário e não enviar o PAN através de e-mails não codificados.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **3.1** Mantenha a informação armazenada do portador de cartão em um tamanho mínimo. Desenvolva uma política de retenção e destruição de dados. Limite o tempo e a quantidade de dados retidos exclusivamente para o que é necessário ao negócio e com propósitos legais e/ou regulamentares, conforme documentado no regulamento de retenção de dados. | **3.1** Obtenha e examine as políticas e procedimentos da empresa referentes à retenção e destruição de dados, e faça o seguinte:<br>• Verifique se as políticas e procedimentos incluem as exigências legais, regulamentares e do negócio para a retenção de dados, incluindo as exigências específicas para os dados do portador de cartão (por exemplo, os dados do portador de cartão precisam ser mantidos por um período X por razões de negócio Y)<br>• Verifique se as políticas e procedimentos incluem artigos relativos à disposição dos dados quando não mais necessários por razão legal, regulamentar ou de negócio, incluindo a disposição dos dados dos portadores de cartão<br>• Verifique se as políticas e procedimentos incluem cobertura para toda a armazenagem dos dados dos portadores de cartão, incluindo os servidores do banco de dados, mainframes, transferência de diretórios e cópia em massa dos diretórios usados para transferir dados entre servidores e diretórios usados para normalizar os dados entre as transferências de servidor | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | • Verifique se as políticas e procedimentos incluem um processo programático (automático) para remover, pelo menos em bases trimestrais, os dados dos portadores de cartão armazenados que excedam as exigências de retenção do negócio, ou, alternativamente, a realização de uma auditoria, pelo menos trimestralmente, para verificar se os dados armazenados dos portadores de cartão não ultrapassam as exigências de retenção do negócio | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **3.2** Não armazene dados confidenciais de autenticação após a autorização (nem mesmo codificados).<br>Os dados confidenciais de autenticação incluem os dados mencionados nas Exigências 3.2.1 a 3.2.3 a seguir*:* | **3.2** Se os dados confidenciais de autenticação forem recebidos e apagados, obtenha e revise os processos para a eliminação dos dados para verificar se os dados são irrecuperáveis.<br>Para cada item dos dados confidenciais de autenticação abaixo, execute os seguintes passos: | | | |
| **3.2.1** Não armazene o conteúdo total de qualquer trilha da tarja magnética (no verso de um cartão, em um chip ou em qualquer outro lugar). Estes dados são alternativamente chamados de dados da trilha completa, trilha, trilha 1, trilha 2 e tarja magnética<br>*No curso normal do negócio, os seguintes elementos dos dados da tarja magnética podem ser necessários reter: o nome do titular da conta,o número da conta primária (PAN), a data de vencimento e o código de serviço. Para minimizar o risco, armazene apenas os elementos dos dados necessários ao negócio. NUNCA guarde os elementos dos dados do código ou valor de verificação ou valor de verificação do PIN.*<br>*Nota: Consultar o "Glossário" para informações adicionais.* | **3.2.1** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, examine o seguinte e certifique-se de que o conteúdo completo de qualquer trilha da tarja magnética no verso do cartão não é armazenado sob qualquer circunstância:<br>• Dados de entrada da transação<br>• Registros das transações<br>• Arquivos de histórico<br>• Trace files<br>• Registros de debugging<br>• Diversos esquemas de bancos de dados<br>• Conteúdo do banco de dados | | | |
| **3.2.2** Não armazene o valor ou código de validação do cartão (valor de três ou quatro dígitos impressos na frente ou verso de um cartão de | **3.2.2** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, examine o seguinte e verifique se o código de validação de três ou quatro dígitos impresso na frente do cartão ou no painel | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| pagamento) usado para verificar as transações com cartão não presente<br>*Nota: Consultar o "Glossário" para informações adicionais.* | de assinatura (dados do CVV2, CVC2, CID, CAV2) não está armazenado sob qualquer circunstância:<br>• Dados de entrada da transação<br>• Registros das transações<br>• Arquivos de histórico<br>• Trace files<br>• Registros de debugging<br>• Diversos esquemas de bancos de dados<br>• Conteúdo do banco de dados | | | |
| **3.2.3** Não armazene o número de identificação pessoal (PIN) ou o bloqueador do PIN codificado. | **3.2.3** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso, examine o seguinte e certifique-se de que os PINs e os o bloqueadores do PIN codificado não são armazenados sob qualquer circunstância:<br>• Dados de entrada da transação<br>• Registros das transações<br>• Arquivos de histórico<br>• Trace files<br>• Registros de debugging<br>• Diversos esquemas de bancos de dados<br>• Conteúdo do banco de dados | | | |
| **3.3** Oculte o PAN quando exibido (os primeiros seis e os quatro últimos dígitos são o maior número de dígitos que devem ser mostrados).<br>*Nota: Esta exigência não se aplica àqueles funcionários e outros que possuam a necessidade específica de ver o PAN completo; também não substitui exigências mais rígidas em vigor para a exibição dos dados do portador de cartão (por exemplo, para os comprovantes do ponto de venda [POS]).* | **3.3** Obtenha e examine as políticas escritas e os displays on-line dos dados do cartão de crédito para certificar-se de que os números dos cartões de crédito estejam disfarçados quando mostrando os dados do portador de cartão, exceto quando houver a necessidade específica de consultar a totalidade dos números do cartão de crédito | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **3.4** Tornar, no mínimo, o PAN ilegível em qualquer local em que as mesmas sejam armazenadas (incluindo os dados em mídia portátil, mídia de back-up, em relatórios e dados recebidos ou armazenados por redes wireless) através do uso de qualquer uma das seguintes técnicas:<br>• Funções rigorosas de one-way hash (hashed indexes)<br>• Truncagem<br>• Index tokens e pads (os pads devem ser armazenados com segurança)<br>• Codificação forte associada com processos chave de administração e procedimentos<br>A informação MÍNIMA da conta que deve ser tornada ilegível é o PAN.<br>*Se, por alguma razão, a companhia não for capaz de codificar os dados do portador de cartão, consulte o Anexo B: "Controles de Compensação."* | **3.4.a** Obtenha e examine a documentação sobre o sistema usado para proteger os dados armazenados, incluindo o prestador de serviço, tipo de sistema/processo e os algoritmos de codificação (se aplicável). Verifique se os dados foram tornados ilegíveis através do uso de um dos seguintes métodos:<br>• One-way hashes (hashed indexes) tais como SHA-1<br>• Truncagem ou masking<br>• Index tokens e PADs, com os PADs sendo armazenados de forma segura<br>• Codificação rigorosa, tal como Triple-DES 128-bit ou AES 256-bit, associada com os processos e procedimentos de administração de chave | | | |
| | **3.4.b** Examine diversas tabelas de uma amostra dos servidores de banco de dados para verificar se os dados são tornados ilegíveis (ou seja, não armazenados em texto pleno) | | | |
| | **3.4.c** Examine uma amostra da mídia removível (por exemplo, fitas de back-up) para confirmar se os dados dos portadores de cartão são tornados ilegíveis | | | |
| | **3.4.d** Examine uma amostra dos logs de auditoria e confirme se os dados dos portadores de cartão para confirmar se os dados dos portadores de cartão são depurados ou removidos dos logs | | | |
| | **3.4.e** Verifique se os dados dos portadores de cartão recebido através da rede são tornados ilegíveis sempre que armazenados | | | |
| **3.4.1** Se a codificação do disco for usada (em vez da codificação do banco de dados a nível de coluna ou arquivo), o acesso lógico deve ser administrado independentemente dos | **3.4.1.a** Se a codificação do disco for usada, verifique se o acesso lógico aos sistemas do arquivo codificado está implementado através de um mecanismo que é separado do mecanismo dos sistemas operacionais nativos (por exemplo, não usando o sistema local ou as contas do Diretório Ativo) | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| mecanismos de controle de acesso ao sistema operacional nativo (por exemplo, não usando o sistema local ou as contas do Diretório Ativo). A descrição das chaves não deve ser ligada às contas dos usuários. | **3.4.1.b** Verifique se as chaves de codificação não estão armazenadas no sistema local (por exemplo, armazene as chaves em um floppy disk, CD-ROM, etc. para que as mesmas estejam seguras e possam ser recuperadas apenas quando se fizer necessário) | | | |
| | **3.4.1.c** Verifique se os dados do portador de cartão na mídia removível estão codificados sempre que forem armazenados (a codificação do disco geralmente não pode codificar a mídia removível) | | | |
| **3.5** Proteja as chaves de codificação contra a divulgação e o uso indevido: | **3.5** Verifique os processos para a proteção das chaves usadas para codificação dos dados do portador de cartão contra a divulgação e uso indevido fazendo o seguinte: | | | |
| **3.5.1** Restrinja o acesso às chaves ao menor número de custódios necessários | **3.5.1** Examine as listas de acesso pelo usuário para certificar-se de que o acesso às chaves de codificação seja restrito a muito poucos custódios | | | |
| **3.5.2** Guarde as chaves de forma segura no menor número de modalidades e lugares | **3.5.2** Examine os arquivos de configuração do sistema para verificar se as chaves de codificação estão armazenadas em formato codificado e se as chaves de codificação das chaves estão armazenas separadamente das chaves de codificação de dados | | | |
| **3.6** Documente completamente e implemente todos os processos e procedimentos de administração das chaves usados para a codificação dos dados, incluindo o seguinte: | **3.6.a** Verifique a existência de procedimentos para a administração de chave para as chaves usadas para a codificação dos dados do portador de cartão | | | |
| | **3.6.b** **Para os Prestadores de Serviço** apenas: Se o Prestador de Serviço compartilha as chaves com seus clientes para a transmissão de dados dos portadores de cartão, verifique se o Prestador de Serviço oferece uma documentação aos clientes que inclua orientação sobre como armazenar com segurança e mudar as chaves de codificação dos clientes (usado para transmitir os dados entre o cliente e o prestador de serviço) | | | |
| | **3.6.c** Examine os procedimentos de administração de chave e faça o seguinte: | | | |
| **3.6.1** Geração de chaves fortes | **3.6.1** Verifique se os procedimentos de administração de chave exigem a geração de chaves fortes | | | |
| **3.6.2** Distribuição segura de chaves | **3.6.2** Verifique se os procedimentos de administração de chave exigem a distribuição segura das chaves | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **3.6.3** Armazenagem segura das chaves | **3.6.3** Verifique se os procedimentos de administração de chave exigem a armazenagem segura das chaves | | | |
| **3.6.4** Mudança periódica das chaves<br>• De acordo com o necessário e recomendado pelo aplicativo associado (por exemplo, re-keying); de preferência automaticamente<br>• Pelo menos uma vez por ano | **3.6.4** Verifique se os procedimentos de administração de chave exigem mudanças periódicas das chaves. Verifique se os procedimentos de mudança das chaves são realizados pelo menos uma vez por ano | | | |
| **3.6.5** Destruição das chaves antigas | **3.6.5** Verifique se os procedimentos de administração de chave exigem a destruição das chaves antigas | | | |
| **3.6.6** Conhecimento compartilhado e estabelecimento de controle duplo das chaves (sendo necessária a existência de duas ou três pessoas, cada uma conhecendo apenas a sua parte da chave, para reconstruir a chave inteira) | **3.6.6** Verifique se os procedimentos de administração de chave exigem conhecimento compartilhado e controle duplo das chaves (sendo necessária a existência de duas ou três pessoas, cada uma conhecendo apenas a sua parte da chave, para reconstruir a chave inteira) | | | |
| **3.6.7** Prevenção contra a substituição não autorizada das chaves | **3.6.7** Verifique se os procedimentos de administração de chave exigem a prevenção contra a substituição não autorizada das chaves | | | |
| **3.6.8** Reposição das chaves conhecidas ou com suspeita de comprometimento | **3.6.8** Verifique se os procedimentos de administração de chave exigem a reposição das chaves conhecidas ou suspeitas de comprometimento | | | |
| **3.6.9** Cancelamento das chaves antigas ou inválidas | **3.6.9** Verifique se os procedimentos de administração de chave exigem o cancelamento das chaves antigas ou inválidas (principalmente as chaves RSA) | | | |
| **3.6.10** Exigência de que os custódios das chaves assinem um documento especificando que eles compreendem e aceitam as responsabilidades de custódios das chaves | **3.6.10** Verifique se os procedimentos de administração de chave exigem que os custódios das chaves assinem um documento especificando que eles compreendem e aceitam as suas responsabilidades de custódios das chaves | | | |

## Exigência 4: Codifique a transmissão dos dados do portador de cartão nas redes públicas e abertas

As informações confidenciais devem ser codificadas durante a transmissão através das redes que são facilmente e comumente interceptadas, modificadas ou redirecionadas por um hacker quando em trânsito.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **4.1** Use protocolos de codificação e cifragem rigorosos tais como secure sockets layer (SSL) / transport layer security (TLS) e internet protocol security (IPSEC) para proteger os dados confidenciais do portador de cartão durante a transmissão através das redes públicas e abertas.<br>*Exemplos de redes públicas e abertas que estão no âmbito do PCI DSS são a Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM) e general packet radio service (GPRS).* | **4.1.a** Verifique o uso da codificação (por exemplo, SSL/TLS ou IPSEC) sempre que os dados dos portadores de cartão forem transmitidos ou recebidos através de redes públicas e abertas<br>• Verifique se é utilizada uma codificação rigorosa durante a transmissão dos dados<br>• Para as implementações de SSL, verifique se o HTTPS aparece como uma parte do browser Universal Record Locator (URL) e que nenhum dado dos portadores de cartão foi solicitado quando o HTTPS não apareceu no URL<br>• Selecione uma amostra das transações como elas são recebidas e observe as transações como elas ocorrem para verificar quais dados dos portadores de cartão foram codificados durante o trânsito<br>• Verifique se apenas as chaves/certificados SSL/TLS são aceitos<br>• Verifique se o rigor adequado da codificação foi implementado para a metodologia de codificação em uso (consulte as recomendações/melhores práticas) | | | |
| **4.1.1 Para as redes wireless transmitindo os dados do portador de cartão**, codifique as transmissões através do uso da tecnologia Wi-Fi protected access (WPA ou WPA2), IPSEC VPN ou SSL/TLS. Nunca confie exclusivamente na wired equivalent privacy (WEP) para proteger a | **4.1.1.a** Para as redes wireless transmitindo os dados dos portadores de cartão ou conectadas aos ambientes do portador de cartão, verifique se as metodologias de codificação são usadas para quaisquer transmissões wireless, tais como: Wi-Fi Protected Access (WPA ou WPA2), IPSEC VPN, ou SSL/TLS | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| confidencialidade e acesso para uma LAN wireless.<br>Se a WEP for usada, faça o seguinte:<br>• Use com uma chave de codificação de, no mínimo, 104-bit e um valor de inicialização de 24 bit<br>• Use APENAS em conjunto com a tecnologia do WiFi protected access (WPA ou WPA2), VPN ou SSL/TLS<br>• Faça a rotação das chaves compartilhadas da WEP trimestralmente (ou automaticamente se a tecnologia permitir)<br>• Faça a rotação das chaves compartilhadas da WEP sempre que houver mudanças no pessoal que tenha acesso às chaves<br>• Restrinja o acesso com base no endereço do código de acesso da mídia | **4.1.1.b** Se a WEP for usada, verifique<br>• se é usada com uma chave de codificação de, no mínimo, 104-bit e um valor de inicialização de 24 bit<br>• se é usada apenas em conjunto com a tecnologia do WiFi protected access (WPA ou WPA2), VPN ou SSL/TLS<br>• se existe a rotatividade das chaves WEP compartilhadas pelo menos trimestralmente (ou automaticamente se a tecnologia permitir)<br>• se existe a rotatividade das chaves WEP compartilhadas sempre que houver mudanças no pessoal que tenha acesso às chaves<br>• se o acesso é restrito com base no endereço do MAC | | | |
| **4.2** Nunca envie PANs não codificados por e-mail. | **4.2.a** Verifique se uma solução de codificação é usada sempre que os dados do portador de cartão forem enviados por e-mail | | | |
| | **4.2.b** Verifique a existência de uma política estipulando que um PAN não codificado não seja enviado por e-mail | | | |
| | **4.2.c** Entreviste de 3 a 5 funcionários para determinar se um software de codificação de e-mails é exigido para os e-mails contendo os PANs | | | |

# Mantenha um Programa de Administração da Vulnerabilidade

## Exigência 5: Use e atualize regularmente o software ou programas antivírus

Muitas das vulnerabilidades e vírus destrutivos entram na rede através das atividades via e-mail dos funcionários. Deve ser usado um software antivírus em todos os sistemas comumente afetados por vírus para protegê-los contra estes softwares destrutivos.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | TARGET DATE/ COMMENTS |
|---|---|---|---|---|
| **5.1** Instale mecanismos antivírus em todos os sistemas comumente afetados por vírus (particularmente computadores pessoais e servidores)<br><br>*Nota: Os sistemas comumente afetados por vírus tipicamente não incluem os sistemas operacionais ou os mainframes com base no UNIX.* | **5.1** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, verifique se um software antivírus foi instalado | | | |
| **5.1.1** Assegure-se de que todos os programas antivírus são capazes de detectar, remover e proteger contra todas as formas de software destrutivo, incluindo spyware e adware. | **5.1.1** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, verifique se programas antivírus detectam, removem e protegem contra software destrutivo, incluindo spyware e adware | | | |

| | | | | |
|---|---|---|---|---|
| **5.2** Assegure-se de que todos os mecanismos antivírus estejam atualizados, rodando ativamente e capazes de gerar logs para auditoria. | **5.2** Para verificar se o software antivírus encontra-se atualizado, rodando ativamente e capaz de gerar logs<br>• Obtenha e examine a política para verificar que a mesma contenha as exigências para a atualização de software antivírus e definições<br>• Verifique se a instalação principal do software habilita as atualizações automáticas e scans periódicos e que uma amostra dos componentes do sistema, servidores críticos e servidores de pontos de acesso possuem estas características habilitadas<br>• Verifique se a geração de log está habilitada e que os logs estejam sendo retidos de acordo com a política de retenção da empresa | | | |

## Exigência 6: Desenvolva e mantenha sistemas e aplicativos seguros

Indivíduos inescrupulosos usam as vulnerabilidades de segurança para obter acesso privilegiado aos sistemas. Muitas destas vulnerabilidades são resolvidas através de patches de segurança do prestador de serviço. Todos os sistemas devem estar com seus patches de software atualizados e adequados para se proteger contra o abuso por parte dos funcionários, hackers externos e vírus. Nota: Os patches apropriados de software são aqueles patches que tenham sido avaliados e testados suficientemente para determinar que os patches não entrem em conflito com as configurações de segurança existentes. Para os aplicativos desenvolvidos in-house, inúmeras vulnerabilidades podem ser evitadas através do uso de processos padrão de desenvolvimento de sistemas e técnicas de codificação seguras.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **6.1** Assegure-se de que todos os componentes do sistema e software possuam instalados os mais recentes patches de segurança fornecidos pelo prestador de serviço. Instale patches de segurança relevantes dentro de um mês após a distribuição. | **6.1.a** Para uma amostra dos componentes do sistema, servidores críticos, pontos de acesso wireless e softwares relacionados, compare a lista dos patches de segurança instalados em cada sistema com a lista mais recente dos patches de segurança do vendedor para determinar se os patches mais atualizados estão instalados | | | |
| | **6.1.b** Examine as políticas relacionadas com a instalação do patch de segurança para verificar se eles exigem a instalação de todos os novos patches de segurança relevantes dentro de 30 dias | | | |
| **6.2** Estabeleça um processo para identificar as vulnerabilidades de segurança recentemente descobertas (por exemplo, assine serviços de alerta disponíveis gratuitamente na Internet). Atualize os padrões para tratar de novos assuntos relacionados com vulnerabilidade. | **6.2.a** Entrevistar o pessoas responsável para verificar se os processos foram implementados de forma a identificar as novas vulnerabilidades de segurança | | | |
| | **6.2.b** Verificar se os processos para identificar as novas vulnerabilidades de segurança incluem o uso de fontes externas para as informações e atualização dos padrões de configuração do sistema revistos na Exigência 2 à medida que novos assuntos relacionados com vulnerabilidade forem encontrados | | | |
| **6.3** Desenvolva aplicativos de software com base nas melhores práticas da indústria e incorpore a segurança da informação em todo o ciclo de vida do desenvolvimento do software. | **6.3** Obtenha e examine os processos de desenvolvimento de software escritos para verificar se eles estão baseados nos padrões da indústria e que a segurança esteja informação em todo o ciclo de vida<br>A partir do exame dos processos de desenvolvimento de software escritos, de entrevistas com os criadores de software e do exame de dados relevantes | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | (documentação da configuração de network, dados de produção e teste, etc.), verifique se: | | | |
| **6.3.1** Teste todos os sistemas e patches de segurança e as mudanças na configuração do software antes da instalação | **6.3.1** Todas as mudanças (incluindo os patches) foram testadas antes de serem colocadas em produção | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **6.3.2** Mantenha os ambientes de desenvolvimento, teste e produção separados | **6.3.2** Os ambientes de desenvolvimento/teste estão separados do ambiente da produção, com o controle de acesso instalado para reforçar a separação | | | |
| **6.3.3** Separe as responsabilidades entre os ambientes de desenvolvimento, teste e produção | **6.3.3** Existe uma separação de responsabilidades entre o pessoal designado aos ambientes de desenvolvimento/teste e o pessoal designado ao ambiente de produção | | | |
| **6.3.4** Os dados de produção (PANs ativos) não são usados para teste ou desenvolvimento | **6.3.4** Os dados de produção (PANs ativos) não são usados para teste e desenvolvimento ou são sanitizados antes do uso | | | |
| **6.3.5** Remoção dos dados de teste e contas antes que os sistemas de produção se tornem ativos | **6.3.5** Os dados de teste e das contas foram removidos antes de um sistema de produção se tornar ativo | | | |
| **6.3.6** Remoção das contas personalizadas, do nome do usuário e senhas antes que os aplicativos se tornem ativos ou sejam liberados para os clientes | **6.3.6** As contas de aplicação customizadas, nomes de usuários e/ou senhas foram removidas antes do sistema entrar em produção ou ser liberado para os clientes | | | |
| **6.3.7** Revisão dos códigos customizados antes da liberação para a produção ou clientes e para a identificação de qualquer vulnerabilidade potencial do código | **6.3.7.a** Obtenha e revise qualquer política escrita ou outra para confirmar se elas determinam que as revisões de códigos sejam exigidas e devem ser executadas por outros indivíduos que não os autores originais do código | | | |
| | **6.3.7.b** Verifique se as revisões dos códigos estão sendo efetuadas para os novos códigos e após as mudanças nos códigos<br>*Nota: Esta exigência se aplica às revisões do código para o desenvolvimento de software customizado, como parte do System Development Life Cycle (SDLC) – estas revisões podem ser realizadas pelo pessoal interno. O código customizado para aplicativos voltados para a web estará sujeito a controles adicionais em 30 de junho de – consultar a exigência 6.6 do PCI DSS para maiores detalhes.* | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **6.4** Acompanhe as mudanças nos procedimentos de controle de todo o sistema e mudanças na configuração do software. Os procedimentos devem incluir o seguinte: | **6.4.a** Obtenha e examine os procedimentos da empresa com respeito à mudança e controle relacionados com a implementação dos patches de segurança e modificação dos softwares e verifique se os procedimentos exigem os itens de **6.4.1** a **6.4.4** abaixo | | | |
| | **6.4.b** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, examine as três mais recentes mudanças e patches de segurança para cada componente de sistema e investigue estas mudanças de volta à documentação de controle relacionada. Verifique se, para mudança examinada, a seguinte documentação estava de acordo com os procedimentos de controle da mudança: | | | |
| **6.4.1** Documentação do impacto | **6.4.1** Verifique se a documentação do impacto no cliente encontra-se incluída na documentação de controle de mudança para cada amostra de mudança | | | |
| **6.4.2** Administração do “sign-off” para as partes apropriadas | **6.4.2** Verifique se a administração do “sign-off” pelas partes apropriadas encontra-se presente em cada amostra de mudança | | | |
| **6.4.3** Teste da funcionalidade operacional | **6.4.3** Verifique se foi efetuado um teste da funcionalidade operacional para cada amostra de mudança | | | |
| **6.4.4** Procedimentos de back-out | **6.4.4** Verifique se foram preparados os procedimentos de back-out para cada amostra de mudança | | | |
| **6.5** Desenvolva todos os aplicativos de web baseados em diretrizes de codificação seguras, tais como as diretrizes do *Open Web Application Security Project*. Revise o código dos aplicativos customizados para identificar vulnerabilidades. Verifique a prevenção das vulnerabilidades mais comuns nos processos de desenvolvimento do software para incluir o seguinte: | **6.5.a** Obtenha e examine os processos de desenvolvimento de software para quaisquer aplicativos baseados na web. Verifique se os processos requerem um treinamento em técnicas de códigos de segurança para os criadores de aplicativos e que seja baseado em orientação, tais como as diretrizes *OWASP* (http://www.owasp.org) | | | |
| | **6.5.b** Para qualquer aplicativo baseado na web, verifique se os processos estão instalados para confirmar que os aplicativos de web não estejam | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | vulneráveis ao seguinte: | | | |
| **6.5.1** Input não validado | **6.5.1** Input não validado | | | |
| **6.5.2** Quebra do controle de acesso (por exemplo, uso desonesto dos IDs dos usuários) | **6.5.2** Uso desonesto dos IDs dos usuários | | | |
| **6.5.3** Quebra da administração de autenticação e sessão (uso das credenciais da conta e cookies da sessão) | **6.5.3** Uso desonesto das credenciais da conta e cookies da sessão | | | |
| **6.5.4** Ataques ao cross-site scripting (XSS) | **6.5.4** Cross-site scripting | | | |
| **6.5.5** Overflow do buffer | **6.5.5** Overflow do buffer devido a um input não validado e outras causas | | | |
| **6.5.6** Defeitos de injection (por exemplo, structured query language (SQL) injection) | **6.5.6** Defeitos de SQL injection e falha de outros comandos de injeção | | | |
| **6.5.7** Administração incorreta dos erros | **6.5.7** Administração incorreta dos erros | | | |
| **6.5.8** Armazenagem insegura | **6.5.8** Armazenagem insegura | | | |
| **6.5.9** Recusa de serviço | **6.5.9** Recusa de serviço | | | |
| **6.5.10** Administração de configuração insegura | **6.5.10** Administração de configuração insegura | | | |
| **6.6** Assegure-se de que todos os aplicativos voltados para a web estejam protegidos contra ataques conhecidos por um dos seguintes métodos:<br>• Fazer a revisão de todos os códigos de aplicativos customizados para vulnerabilidades comuns por uma organização que se especialize em segurança de aplicativos | **6.6** Para os aplicativos baseados na web, assegure-se de que um dos métodos abaixo esteja instalado como a seguir:<br>• Verifique que o código do aplicativo customizado seja revisado periodicamente por uma organização que se especialize em segurança de aplicativos; que todas as vulnerabilidades dos códigos foram corrigidas; e que o aplicativo foi reavaliado depois das correções | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| • Instalar um firewall application-layer na frente dos aplicativos voltados para a web<br>*Nota: Este método é considerado uma melhor prática até 30 de junho de 2008, e depois se tornará uma exigência.* | • Verifique que um *application-layer firewall* esteja instalado na frente dos aplicativos voltados para a web para detectar e prevenir os ataques com base na web | | | |

# Implemente Medidas Rígidas de Controle de Acesso

## Exigência 7: Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos

Esta exigência assegura que os dados críticos possam apenas ser acessados por pessoas autorizadas.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **7.1** Limite o acesso aos recursos de computação e informação do portador de cartão a apenas aqueles indivíduos cuja execução do trabalho exija tal acesso. | **7.1** Obtenha e examine a política escrita para o controle dos dados e verifique se ela inclui o seguinte:<br>• O acesso aos IDs de usuários privilegiados se encontrem restritos para os mínimos privilégios necessários para a execução das responsabilidades do trabalho<br>• A determinação dos privilégios seja baseada na classificação individual do trabalho e função da pessoa<br>• A exigência de um formulário de autorização assinado pela administração que especifique os privilégios solicitados<br>• A implementação de um sistema de controle de acesso automatizado | | | |
| **7.2** Estabeleça um mecanismo para os sistemas com múltiplos usuários que restrinja o acesso baseado na necessidade de saber do usuário e seja configurado para “negar tudo” a menos que especificamente permitido. | **7.2** Examine a configuração do sistema e documentação do fornecedor para verificar se há um sistema de controle de acesso implementado e se ele inclui o seguinte<br>• Cobertura de todos os componentes do sistema<br>• Determinação dos privilégios a indivíduos com base na classificação do trabalho e função<br>• Configuração padrão para “negar tudo” (alguns sistemas de controle de acesso têm a configuração padrão de “permitir tudo” desta forma permitindo o acesso, a menos que/até que seja escrita uma regra específica para o bloqueio) | | | |

## Exigência 8: Atribua um ID único para cada pessoa que possua acesso ao computador.

Atribuindo uma identificação (ID) única para cada pessoa que possua acesso, assegura que todas as ações tomadas em relação aos dados e sistemas críticos sejam executadas por usuários conhecidos e autorizados, os quais possam ser responsabilizados por estas ações.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **8.1** Identifique todos os usuários com um nome de usuário único antes que os mesmos tenham permissão para acessar os componentes do sistema ou os dados do portador de cartão. | **8.1** Para uma amostra dos IDs dos usuários, faça uma revisão das listas de ID de usuários e verifique se todos os usuários possuem um único nome de usuário para o acesso aos componentes do sistema ou dados dos portadores de cartão | | | |
| **8.2** Além de designar um ID exclusivo, utilize pelo menos um dos métodos abaixo para autenticar todos os usuários:<br>• Senha<br>• Token devices (por exemplo, SecureID, certificados ou chaves públicas)<br>• Biométrica | **8.2** Para verificar se os usuários são validados por intermédio do uso de um ID único e um item adicional de autenticação (por exemplo, uma senha) para ter acesso ao ambiente do portador de cartão, faça o seguinte:<br>• Obtenha e examine a documentação que descreve os métodos de autenticação usados<br>• Para cada tipo de método de autenticação usado para cada tipo de componente de sistema, observe uma autenticação para verificar se o processo está funcionando de acordo com os métodos de autenticação documentados | | | |
| **8.3** Implemente a autenticação por dois fatores para o acesso remoto à rede pelos funcionários, administradores e terceiros. Use tecnologias tais como remote authentication and dial-in service (RADIUS) ou terminal access controller access control system (TACACS) com tokens; ou VPN (com base em SSL/TLS ou IPSEC) com certificados individuais. | **8.3** Para verificar se dois fatores de autenticação estão instalados para todos os acessos remotos à rede, observe um funcionário (por exemplo, um administrador) enquanto ele se conecta remotamente à rede e verifique se tanto a senha como o item adicional de autenticação (Smart card, token PIN) são exigidos. | | | |
| **8.4** Codifique todas as senhas durante a transmissão e armazenagem em todos os componentes do sistema. | **8.4.a** Para uma amostra dos componentes de sistema, servidores críticos e pontos de acesso wireless, examine os arquivos de senha e verifique se as senhas não podem ser lidas | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | **8.4.b** Apenas para os **Prestadores de Serviço**, observe o arquivo de senhas para verificar se as senhas do cliente estão codificadas | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **8.5** Garanta a autenticação eficiente do usuário e a administração da senha para os usuários não consumidores e administradores em todos os componentes do sistema como a seguir: | **8.5** Revise os procedimentos e entreviste o pessoal para verificar se os procedimentos foram implementados para a autenticação do usuário e administração da senha, fazendo o seguinte: | | | |
| **8.5.1** Controle a adição, exclusão e modificação dos IDs dos usuários, credenciais e outros métodos de identificação | **8.5.1.a** Selecione uma amostra dos IDs de usuário, incluindo tanto os administradores como usuários em geral. Verifique se cada usuário está autorizado a usar o sistema de acordo com a política da empresa fazendo o seguinte:<br>• Obtenha um formulário de autorização para cada ID<br>• Verifique se os IDs de Usuário da amostra estão implementados de acordo com o formulário de autorização (incluindo os privilégios de acordo com o especificado e todas as assinaturas obtidas), seguindo a trilha das informações desde o formulário até o sistema | | | |
| | **8.5.1.b** Verifique se apenas os administradores possuem acesso à administração dos consoles das redes wireless | | | |
| **8.5.2** Verifique a identidade do usuário antes de executar a mudança de senhas | **8.5.2** Examine os procedimentos de senha e observe o pessoal de segurança para verificar que, se um usuário solicitar uma mudança na senha via telefone, e-mail, web ou outro método não face a face, a identificação do usuário é verificada antes da alteração na senha | | | |
| **8.5.3** Estabeleça senhas de uso inicial com um valor único por cada usuário e faça uma mudança imediata após ser usada pela primeira vez | **8.5.3** Examine os procedimentos de senha e observe o pessoal de segurança para verificar se as senhas iniciais para os novos usuários são criadas como um valor único para cada usuário e mudadas após o primeiro uso | | | |
| **8.5.4** Revogue imediatamente o acesso para qualquer usuário cancelado | **8.5.4** Selecione a amostra dos funcionários demitidos nos últimos seis meses e faça uma revisão das listas atualizadas de acesso dos usuários para | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | verificar se os seus IDs foram desativados ou removidos | | | |
| **8.5.5** Remova as contas de usuários inativos pelo menos a cada 90 dias | **8.5.5** Para uma amostra dos IDs dos usuários, verifique se não existem contas inativas a mais de 90 dias | | | |
| **8.5.6** Habilite as contas usadas pelos prestadores de serviço para a manutenção remota apenas durante o tempo necessário | **8.5.6** Verifique que quaisquer contas usadas pelos provedores de serviço para dar suporte e fazer a manutenção dos componentes do sistema estejam inativas, habilitadas apenas quando necessário pelo prestador de serviço e monitoradas enquanto estiverem sendo usadas | | | |
| **8.5.7** Comunique os procedimentos e políticas da senha a todos os usuários que tenham acesso aos dados do portador de cartão | **8.5.7** Entreviste os usuários de uma amostra de IDs de usuários para verificar se eles estão familiarizados com os procedimentos e políticas relativos à senha | | | |
| **8.5.8** Não utilize senhas ou contas genéricas de grupo ou compartilhadas | **8.5.8.a** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, examine as listas dos IDs dos usuários para verificar o seguinte<br>• Os IDs genéricos dos usuários e contas foram desativados ou removidos<br>• Os IDs compartilhados de usuários para as atividades de administração do sistema e outras funções críticas não existem<br>• Os IDs compartilhados ou genéricos de usuários não estão sendo usados para administrar a LAN wireless e dispositivos | | | |
| | **8.5.8.b** Examine as políticas/procedimentos de senha e verifique se as senhas de grupo e compartilhadas se encontram explicitamente proibidas | | | |
| | **8.5.8.c** Entreviste os administradores do sistema para verificar se as senhas de grupo e compartilhadas não são distribuídas mesmo quando solicitadas | | | |
| **8.5.9** Mude as senhas dos usuários pelo menos a cada 90 dias | **8.5.9** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a configuração do sistema para verificar se os parâmetros da senha do usuário estão configurados | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | para exigir que os usuários mudem as senhas pelo menos a cada 90 dias<br>Apenas para **Prestadores de Serviço**, faça a revisão dos processos internos e documentação do cliente/usuário para verificar se é exigido que as senhas daquele cliente sejam mudadas periodicamente e que seja dada orientação àqueles clientes de quando e em que circunstâncias as senhas devem ser mudadas | | | |
| **8.5.10** Exija uma senha com o comprimento mínimo de pelo menos sete caracteres | **8.5.10** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a configuração do sistema para verificar se os parâmetros da senha estão ajustados para exigir que as mesmas tenham ao menos o comprimento de sete caracteres<br>Apenas para **Prestadores de Serviço**, faça a revisão dos processos internos e documentação do cliente/usuário para verificar se é exigido que as senhas dos clientes atendam ao comprimento mínimo | | | |
| **8.5.11** Use senhas contendo caracteres tanto numéricos como alfabéticos | **8.5.11** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a definição da configuração do sistema para verificar se os parâmetros da senha estão ajustados para exigir que as senhas contenham caracteres tanto numéricos como alfabéticos<br>Apenas para **Prestadores de Serviço**, faça a revisão dos processos internos e documentação do cliente/usuário para verificar se é exigido que as senhas dos clientes contenham caracteres tanto numéricos como alfabéticos | | | |
| **8.5.12** Não permita que um indivíduo submeta uma nova senha que seja idêntica a qualquer uma das quatro últimas que ele ou ela tenha usado | **8.5.12** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a definição da configuração do sistema para verificar se os parâmetros da senha estão ajustados para exigir que as novas senhas não possam ser idênticas a qualquer uma das quatro senhas anteriormente usadas<br>Apenas para **Prestadores de Serviço**, faça a revisão dos processos internos e documentação do cliente/usuário para verificar se as novas senhas do | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | cliente não possam ser idênticas às quatro senhas anteriores | | | |
| **8.5.13** Limite as tentativas repetidas bloqueando o ID do usuário depois de não mais de seis tentativas | **8.5.13** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a definição da configuração do sistema para verificar se os parâmetros da senha estão ajustados para exigir que uma conta do usuário seja bloqueada depois de não mais de seis tentativas inválidas de logon<br>Apenas para **Prestadores de Serviço**, faça a revisão dos processos internos e documentação do cliente/usuário para verificar se as contas do cliente são temporariamente bloqueadas depois de não mais de seis tentativas inválidas | | | |
| **8.5.14** Ajuste a duração do bloqueio para trinta minutos ou até que o administrador do sistema habilite o ID do usuário | **8.5.14** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a definição da configuração do sistema para verificar se os parâmetros da senha estão ajustados para exigir que uma vez que um usuário seja bloqueado, o mesmo continuará bloqueado por trinta minutos ou até que o administrador do sistema reconfigure a conta | | | |
| **8.5.15** Se uma sessão estiver inativa por mais de 15 minutos, exija que o usuário entre outra vez com a senha para reativar o terminal | **8.5.15** Para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless, obtenha e inspecione a definição da configuração do sistema para verificar se as características do tempo de inatividade do sistema/sessão foram ajustadas para 15 minutos ou menos | | | |
| **8.5.16** Autentique todo o acesso a qualquer banco de dados contendo os dados do portador de cartão. Estes incluem o acesso via aplicativos, administradores e todos os demais usuários | **8.5.16.a** Faça a revisão da configuração dos parâmetros para uma amostra dos bancos de dados para verificar se o acesso é autenticado, inclusive para usuários individuais, aplicativos e administradores | | | |
| | **8.5.16.b** Faça a revisão dos parâmetros da configuração das contas do banco de dados para verificar se as consultas diretas SQL ao banco de dados são proibidas (deve haver muito poucas contas individuais de login no banco de dados. Consultas | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | diretas SQL devem ser limitadas aos administradores do banco de dados) | | | |

## Exigência 9: Restrinja o acesso físico aos dados do portador de cartão

Qualquer acesso físico aos dados ou sistemas que abriguem os dados do portador de cartão cria uma oportunidade para acessar dispositivos ou dados e remover sistemas ou cópias físicas e, portanto devem ser devidamente restritos

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **9.1** Use os controles adequados para a admissão nas instalações para limitar e monitorar o acesso físico aos sistemas que armazenam, processam ou transmitem os dados do portador de cartão. | **9.1** Verifique a existência de controles de segurança física para cada sala de computador, centro de dados e outras áreas físicas com sistemas que contenham os dados dos portadores de cartão<br>• Verifique se o acesso é controlado via leitoras de crachá e outros dispositivos incluindo crachás autorizados, trancas e chaves<br>• Observe uma tentativa do administrador do sistema em fazer o log nos consoles para três sistemas selecionados randomicamente no ambiente do portador de cartão e verifique se eles estão "bloqueados" para prevenir o uso não autorizado | | | |
| **9.1.1** Use câmeras para monitorar áreas críticas. Faça a auditoria dos dados coletados e faça a correlação com outras entradas. Armazene estes dados pelo menos por três meses, a menos que seja proibido por lei. | **9.1.1** Verifique se câmeras de vídeo monitoram os pontos de entrada e saída dos centros de dados onde os dados dos portadores de cartão são armazenados ou estão presentes. As câmeras de vídeo devem estar no interior do centro de dados ou protegidas contra ataque ou desativação. Verifique se as câmeras estão monitoradas e se os dados das câmeras são armazenados pelo menos por três meses | | | |
| **9.1.2** Restrinja o acesso físico às tomadas de acesso público à rede | **9.1.2** Verifique através de entrevistas com os administradores da rede e por observação se as tomadas da rede estão habilitadas apenas quando necessário a funcionários autorizados. Por exemplo, as salas de conferência usadas por visitantes não devem ter uma rede de ports habilitada com DHCP. Alternativamente, verifique se os visitantes são acompanhados todo o tempo nas áreas com uma rede ativa de tomadas | | | |
| **9.1.3** Restrinja o acesso físico a pontos de acesso wireless, gateways e dispositivos portáteis | **9.1.3** Verifique se o acesso físico a pontos de acesso wireless, gateways e dispositivos portáteis encontra-se propriamente restrito | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **9.2** Desenvolva procedimentos para auxiliar todo o pessoal a facilmente distinguir entre funcionários e visitantes, especialmente nas áreas onde os dados do portador de cartão podem ser acessados.<br>*"Funcionário" se refere a empregados de meio expediente e tempo integral, temporários, estagiários e consultores que são "residentes" na instalação da empresa. Um "visitante" é definido como um fornecedor, convidado de um funcionário, pessoal de manutenção e serviço ou qualquer um que necessite entrar nas instalações por um curto período de tempo, geralmente por não mais do que um dia.* | **9.2.a** Faça a revisão dos processos e procedimentos para designar crachás aos funcionários, prestadores de serviços e visitantes e verifique se estes processos incluem o seguinte:<br>• Procedimentos instalados para designar novos crachás, exigências para mudanças de acesso e cancelamento dos crachás vencidos de visitantes e de funcionários demitidos<br>• Acesso limitado ao sistema de crachás | | | |
| | **9.2.b** Observe as pessoas dentro das instalações para verificar se é fácil distinguir entre funcionários e visitantes | | | |
| **9.3** Certifique-se de que todos os visitantes são administrados como a seguir: | **9.3** Verifique se os controles para funcionário/visitante estão instalados como a seguir: | | | |
| **9.3.1** São autorizados antes de entrar nas áreas onde os dados do portador de cartão são processados ou mantidos | **9.3.1** Observe os visitantes para verificar o uso dos crachás de ID de visitante. Tente obter o acesso ao centro de dados para verificar se um crachá de ID de visitante não permite o acesso desacompanhado a áreas físicas que armazenem os dados dos portadores de cartão | | | |
| **9.3.2** Recebam uma identificação física (por exemplo, um crachá ou dispositivo de acesso) que tenha vencimento e que os identifique como não funcionários | **9.3.2** Examine os crachás dos funcionários e visitantes para verificar se os crachás de ID distinguem claramente os funcionários dos visitantes/estranhos e que os crachás dos visitantes tenham um vencimento | | | |
| **9.3.3** Sejam solicitados a retornar a identificação física antes de deixar a instalação ou na data do vencimento | **9.3.3** Observe os visitantes deixando a instalação para verificar se é solicitado que os mesmos devolvam os seus crachás de ID na hora da saída ou no vencimento | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **9.4** Use um registro de visitantes para manter uma evidência física de auditoria da atividade do visitante. Conserve este registro no mínimo por três meses, a menos que proibido por lei. | **9.4.a** Verifique se um log de visitante se encontra em uso para registrar o acesso físico às instalações bem como para as salas dos computadores e centro de dados onde os dados dos portadores de cartão são armazenados ou transmitidos | | | |
| | **9.4.b** Verifique se o log contém o nome do visitante, o nome da empresa representada, o nome do funcionário autorizando o acesso físico e que seja retido pelo menos por três meses | | | |
| **9.5** Armazene os back-ups da mídia em um local seguro, de preferência em uma instalação externa, tal como um local alternativo ou de back-up, ou uma instalação comercial de armazenagem. | **9.5** Verifique se o local de armazenagem para os back-ups da mídia é seguro. Verifique se o local externo de armazenagem é visitado periodicamente para determinar se a armazenagem da mídia de back-up é fisicamente segura e à prova de incêndio | | | |
| **9.6** Exerça a segurança física de toda a mídia de papel e eletrônica (incluindo computadores, mídia eletrônica, hardware de rede e comunicação, linhas de telecomunicação, recibos em papel, relatórios em papel e faxes) que contenham dados do portador de cartão | **9.6** Verifique se os procedimentos para a proteção dos dados do portador de cartão incluem os controles para assegurar fisicamente a mídia em papel e eletrônica nas salas do computador e centros de dados (incluindo recibos em papel, relatórios em papel, faxes, CDs e discos nas mesas dos funcionários, espaços abertos de trabalho e hard drives dos PCs) | | | |
| **9.7** Mantenha um controle rigoroso sobre a distribuição interna ou externa de qualquer tipo de mídia que contenha dados do portador de cartão, incluindo o seguinte: | **9.7** Verifique se existe uma política para controlar a distribuição da mídia contendo os dados do portador de cartão, e que a política cubra todas as mídias distribuídas, incluindo aquelas distribuídas a indivíduos | | | |
| **9.7.1** Classifique a mídia de forma que a mesma possa ser identificada como confidencial | **9.7.1** Verifique se toda a mídia deve ser classificada de forma a que possa ser identificada como “confidencial” | | | |
| **9.7.2** Envie a mídia por intermédio de um mensageiro seguro ou um mecanismo de entrega que possa ser acompanhado de forma precisa | **9.7.2** Verifique se todas as mídias enviadas para fora das instalações são registradas e autorizadas pela administração e enviadas via um mensageiro seguro ou outro mecanismo de entrega que possa ser acompanhado | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **9.8** Obtenha a aprovação da administração para qualquer mídia que seja transportada para fora da área de segurança (especialmente quando a mídia for distribuída para indivíduos). | **9.8** Selecione uma amostra recente de diversos dias dos logs de acompanhamento da mídia externa e verifique a presença no registro dos detalhes de acompanhamento e a devida autorização pela administração | | | |
| **9.9** Mantenha um controle rigoroso sobre a armazenagem e acesso à mídia que contenha dados do portador de cartão. | **9.9** Obtenha e examine a política para o controle da armazenagem e manutenção da mídia em cópia física e eletrônica e verifique se esta política exige inventários periódicos da mídia. | | | |
| **9.9.1** Faça um inventário rigoroso de toda a mídia e certifique-se de que a mesma está armazenada de forma segura. | **9.9.1.a** Obtenha e faça a revisão do log do inventário da mídia para verificar se os inventários periódicos da mídia são efetuados<br>**9.9.1.b** Faça a revisão dos processos para verificar se a mídia se encontra seguramente armazenada | | | |
| **9.10** Destrua a mídia contendo os dados do portador de cartão quando não for mais necessária para o negócio ou por razões legais como a seguir: | **9.10** Obtenha e examine a política de destruição periódica de mídia e verifique se ela cobre todas as mídias que contenham dados dos portadores de cartão e confirme o seguinte: | | | |
| **9.10.1** Corte no sentido cruzado com picotador de papel, incinere ou reduza à polpa os materiais de cópia física | **9.10.1.a** Verifique se os materiais em cópia física são picotados no sentido cruzado, incinerados, ou reduzidos à polpa, de acordo com ISO 9564-1 ou ISO 11568-3e | | | |
| | **9.10.1.b** Examine os receptáculos de armazenamento da informação a ser destruída e verifique se os mesmos são seguros. Por exemplo, verifique que um receptáculo 'a ser picotado' tenha uma tranca que impeça o acesso ao seu conteúdo | | | |
| **9.10.2** Purgue, neutralize, picote ou destrua de outra forma a mídia eletrônica de maneira a que os dados do portador de cartão não possam ser reconstruídos | **9.10.2** Verifique se a mídia eletrônica é destruída além de qualquer recuperação através do uso de um programa militar de remoção de arquivo ou via um processo de degaussing ou destruição física da mídia | | | |

# Acompanhe e Teste Regularmente as Redes

## Exigência 10: Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.

Os mecanismos de registro (logs) e a habilidade de acompanhar as atividades do usuário são fundamentais. A presença dos registros em todos os ambientes permite o acompanhamento preciso e a análise quando algo de errado acontece. A determinação da causa de um comprometimento se torna muito difícil sem os registros das atividades do sistema.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTIE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **10.1** Estabeleça um processo para vincular todo o acesso aos componentes do sistema (especialmente aqueles feitos com privilégios administrativos tais como raiz (root)) para cada usuário individual. | **10.1** Verifique, através de observação e entrevista com o administrador do sistema, se os registros de auditoria estão habilitados e ativos, inclusive para qualquer rede wireless conectada. | | | |
| **10.2** Implemente os registros de auditoria automatizados para reconstruir os seguintes eventos: | **10.2** Verifique, através de entrevista, revisão dos registros de auditoria e exame das configurações do registro de auditoria, se os eventos a seguir constam dos registros de atividade do sistemas: | | | |
| **10.2.1** Todos os acesso individuais feitos aos dados do portador de cartão | **10.2.1** Todos os acessos individuais feitos aos dados do portador de cartão | | | |
| **10.2.2** Todas as ações tomadas por qualquer indivíduo com privilégios tipo “root” ou administrativos | **10.2.2** Todas as ações tomadas por qualquer indivíduo com privilégios tipo “root” ou administrativos | | | |
| **10.2.3** Acesso a todos os registros de auditoria | **10.2.3** Acesso a todos os registros de auditoria | | | |
| **10.2.4** Tentativas de acesso lógico inválidas | **10.2.4** Tentativas de acesso lógico inválidas | | | |
| **10.2 5** Uso de mecanismos de identificação e autenticação | **10.2.5** Uso de mecanismos de identificação e autenticação | | | |
| **10.2.6** Inicialização dos logs de auditoria | **10.2.6** Inicialização dos logs de auditoria | | | |
| **10.2.7** Criação ou eliminação de objetos ao nível de sistema | **10.2.7** Criação ou eliminação de objetos ao nível de sistema | | | |
| **10.3** Grave pelo menos as seguintes entradas nos registros de auditoria para cada evento ligado a todos os componentes do sistema: | **10.3** Verifique através de entrevistas e observação, para cada evento auditável mencionado (no item 10.2), se o registro de auditoria captura o seguinte: | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTIE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **10.3.1** Identificação do usuário | **10.3.1** Identificação do usuário | | | |
| **10.3.2** Tipo de evento | **10.3.2** Tipo de evento | | | |
| **10.3.3** Data e hora | **10.3.3** Carimbo da data e hora | | | |
| **10.3.4** Indicação de sucesso ou falha | **10.3.4** Indicação de sucesso ou falha, incluindo aqueles para as conexões wireless | | | |
| **10.3.5** Origem do evento | **10.3.5** Origem do evento | | | |
| **10.3.6** Identidade ou nome dos dados, componentes do sistema ou recursos afetados | **10.3.6** Identidade ou nome dos dados, componentes do sistema ou recursos afetados | | | |
| **10.4** Sincronize todos os relógios e horas de todos os sistemas críticos | **10.4** Obtenha e faça a revisão dos processos para receber e distribuir a hora correta dentro da organização, assim como as configurações dos parâmetros do sistema relacionados com tempo para uma amostra dos componentes do sistema, servidores críticos e pontos de acesso wireless. Verifique se no processo o seguinte está incluído e implementado: | | | |
| | **10.4.a** Verifique se o NTP ou tecnologia similar é usada para a sincronização da hora | | | |
| | **10.4.b** Verifique se os servidores internos não estão todos recebendo sinais de hora de fontes externas. [Dois ou três servidores de hora central dentro da organização recebem sinais externos de hora [diretamente de um radio especial, satélites GPS ou outras fontes externas com base no Tempo Atômico Internacional e UTC (antigo GMT)], em par com outros para manter o horário preciso e compartilhá-lo com os outros servidores internos] | | | |
| | **10.4.c** Verifique se o Network Time Protocol (NTP) está rodando a versão mais recente | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTIE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | **10.4.d** Verifique se estão designados hosts externos específicos dos quais o servidor de hora irá aceitar as atualizações de hora NTP (para evitar que um atacante mude o relógio). Opcionalmente, estas atualizações podem ser codificadas com uma chave simétrica e podem ser criadas listas de acesso que especifiquem o endereço de IP das máquinas dos clientes que receberão o serviço NTP (para prevenir o uso não autorizado dos servidores internos de hora).<br>Consulte o www.ntp.org para maiores informações | | | |
| **10.5** Torne seguros os registros de auditoria de forma a que eles não possam ser alterados | **10.5** Entreviste o administrador do sistema e examine as permissões para verificar se os registros de auditoria estão seguros de forma a que eles não possam ser alterados como a seguir: | | | |
| **10.5.1** Limite o acesso aos registros de auditoria àqueles que tenham necessidade relacionada com o trabalho | **10.5.1** Verifique se apenas os indivíduos que possuem uma necessidade relacionada com o trabalho têm acesso aos arquivos de registro da auditoria | | | |
| **10.5.2** Proteja os arquivos contendo os registros de auditoria contra modificações não autorizadas | **10.5.2** Verifique se os arquivos atualizados do registro de auditoria estão protegidos contra modificações não autorizadas via mecanismos de controle do acesso, separação física e/ou separação da rede | | | |
| **10.5.3** Faça o back-up imediato dos arquivos contendo os registros de auditoria em um servidor centralizado de logs ou mídia que seja difícil de alterar | **10.5.3** Verifique se os arquivos atualizados do registro de auditoria têm o seu back-up imediato em um servidor centralizado de registros ou mídia que seja difícil de alterar | | | |
| **10.5.4** Copie os registros das redes wireless em um servidor de registro na LAN interna | **10.5.4** Verifique se registros das redes wireless são descarregados ou copiados em um servidor interno centralizado de log ou mídia que seja difícil de alterar | | | |
| **10.5.5** Use um software de acompanhamento e detecção de mudanças na integridade dos arquivos nos registros de forma a assegurar que os dados dos registros existentes não possam ser alterados sem gerar alertas (embora a | **10.5.5** Verifique o uso da monitoração da integridade de arquivo ou software de detecção de mudança de registros através da observação dos parâmetros do sistema e os arquivos monitorados, bem como os resultados das atividades de acompanhamento | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTIE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| adição de um novo dado não deva causar um alerta) | | | | |
| **10.6** Revise os registros de todos os componentes do sistema pelo menos diariamente. A revisão dos registros deve incluir aqueles servidores que executam funções de segurança tais como os servidores de intrusion detection system (IDS) e authentication, authorization and accounting protocol (AAA), por exemplo, RADIUS.<br>*Nota: As ferramentas de busca de registro, análise e alerta podem ser usadas para atender à compliance com a Exigência 10.6* | **10.6.a** Obtenha e examine as políticas de segurança e procedimentos para verificar se elas incluem os procedimentos para a revisão da segurança dos registros pelo menos diariamente e que seja necessário um follow-up das exceções | | | |
| | **10.6.b** Através de observação e entrevistas, verifique se são executadas revisões regulares dos registros para todos os componentes do sistema | | | |
| **10.7** Mantenha o histórico do registro de auditoria por pelo menos um ano, com um mínimo de três meses disponível on-line. | **10.7.a** Obtenha e examine as políticas de segurança e procedimentos e verifique se elas incluem a auditoria das políticas de retenção de registros e exigem a retenção do registro de auditoria pelo menos por um ano | | | |
| | **10.7.b** Verifique se os registros de auditoria se encontram disponíveis on-line ou em fita por um período de pelo menos um ano | | | |

## Exigência 11: Teste regularmente os sistemas e processos de segurança.

As vulnerabilidades são continuamente descobertas por hackers e pesquisadores e introduzidas por novos softwares. Os sistemas, processos e softwares customizados devem ser testados freqüentemente para garantir que a segurança está sendo mantida ao longo do tempo e através das mudanças nos softwares.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATE ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **11.1** Faça os testes dos controles de segurança, das limitações, das conexões com a rede e das restrições anualmente, para certificar-se de que eles podem ser identificados adequadamente e cancelar quaisquer tentativas de acesso não autorizado. Use um analisador de wireless pelo menos trimestralmente para identificar todos os dispositivos wireless em uso. | **11.1.a** Confirme através de entrevista com o pessoal de segurança e examinando os códigos relevantes, documentação e processos que os testes de seguranças dos dispositivos estão instalados para se assegurar de que os controles identificam e cancelam as tentativas não autorizadas dentro do ambiente do portador de cartão. | | | |
| | **11.1.b** Verifique se um analisador de wireless é utilizado pelo menos trimestralmente para identificar os dispositivos wireless. | | | |
| **11.2** Execute scans para testar a vulnerabilidade interna e externa da rede pelo menos trimestralmente e após qualquer mudança significativa na rede (tais como a instalação de um novo componente de sistema, mudanças na topologia da rede, modificações na regra do firewall, upgrades de produtos).<br>*Nota: Trimestralmente, os scans de vulnerabilidade externa devem ser executados por um prestador de serviço de scan qualificado pela indústria de cartões de pagamentos. Os scans realizados após as mudanças na rede podem ser executados pelo pessoal interno da companhia.* | **11.2.a** Inspecione os outputs nos quatro trimestres mais recentes da rede, host e scans da vulnerabilidade do aplicativo para verificar se foram feitos testes periódicos dos dispositivos dentro do ambiente do portador de cartão. Confirme se o processo de scan inclui rescans até que seja obtido um resultado satisfatório (clean) | | | |
| | **11.2.b** Para verificar se um scan externo está sendo feito trimestralmente de acordo com os Procedimentos de Scanning de Segurança da PCI, inspecione o resultado dos quatro trimestres mais recentes de scan de vulnerabilidades externas para verificar se:<br>• Foram feitos quatro scans trimestrais no período dos 12 meses mais recentes<br>• Os resultados de cada scan satisfizeram os Procedimentos de Scanning de Segurança da PCI (por exemplo, nenhuma vulnerabilidade urgente, crítica ou alta)<br>• Os scans foram completados por um | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATE ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | prestador de serviço aprovado para executar os Procedimentos de Scanning de Segurança da PCI | | | |
| **11.3** Execute um teste de penetração pelo menos uma vez por ano e após qualquer modificação ou upgrade significativo da infra-estrutura ou aplicativo (tais como um upgrade do sistema operacional, adição de uma sub-rede no ambiente, adição de um servidor de web no ambiente). Estes testes de penetração devem incluir o seguinte: | **11.3** Obtenha e examine os resultados do mais recente teste de penetração para verificar se o mesmo é feito pelo menos uma vez por ano e após qualquer mudança significativa no ambiente. Verifique se qualquer vulnerabilidade encontrada foi corrigida. Verifique se os testes de penetração incluem: | | | |
| **11.3.1** Testes de penetração do tipo network-layer | **11.3.1** Testes de penetração do tipo network-layer | | | |
| **11.3.2** Testes de penetração do tipo application-layer | **11.3.2** Testes de penetração do tipo application-layer | | | |
| **11.4** Use sistemas de detecção de intrusão na rede, sistemas de detecção baseados em host e sistemas de prevenção de intrusão para acompanhar todo o tráfego na rede e alertar os funcionários para suspeitas de comprometimentos. Mantenha atualizados todos os sistemas de detecção e prevenção. | **11.4.a** Observe o uso do detector de intrusão nos sistemas da rede e/ou sistema prevenção de intrusão na rede. Verifique se todo o tráfego crítico da rede no ambiente dos dados do portador de cartão está monitorado | | | |
| | **11.4.b** Confirme se IDS e/ou IPS se encontram instalados para monitorar e alertar os funcionários sobre suspeitas de comprometimentos | | | |
| | **11.4.c** Examine as configurações de IDS/IPS e confirme se estes dispositivos encontram-se configurados, mantidos e atualizados conforme as instruções do fornecedor para proporcionar o máximo de proteção | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATE ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **11.5** Instale o acompanhamento da integridade de arquivos para alertar os funcionários sobre uma modificação não autorizada de sistemas críticos ou conteúdo de arquivos e execute as comparações destes arquivos críticos pelo menos semanalmente.<br>*Os arquivos críticos não são necessariamente apenas aqueles que contêm os dados do portador de cartão. Com relação ao acompanhamento da integridade dos arquivos críticos, são considerados geralmente arquivos críticos aqueles que não mudam regularmente, mas a modificação pode indicar um comprometimento ou risco de comprometimento do sistema. Os produtos de acompanhamento da integridade de arquivo geralmente vêm pré-configurados com os arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, tais como aqueles de aplicativos customizados, devem ser avaliados e definidos pela entidade (que pode ser o estabelecimento ou prestador de serviço)* | **11.5** Verifique o uso dos produtos de acompanhamento da integridade de arquivos dentro do ambiente dos dados do portador de cartão através da inspeção dos parâmetros do sistema e dos arquivos monitorados, bem como da revisão dos resultados das atividades monitoradas | | | |

# Mantenha uma Política de Segurança da Informação

## Exigência 12: Mantenha uma política que atenda à segurança da informação para funcionários e prestadores de serviços.

Uma política rigorosa de segurança cria um exemplo para toda a empresa e informa os funcionários sobre o que é esperado deles. Todos os funcionários devem estar cientes do cuidado a ter com os dados e suas responsabilidades em protegê-los.

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **12.1** Estabeleça, divulgue, mantenha e dissemine uma política de segurança que: | **12.1** Examine a política de segurança da informação e verifique se a mesma é divulgada e disseminada para todos os usuários relevantes do sistema (incluindo os fornecedores, prestadores de serviços e parceiros de negócio) | | | |
| **12.1.1** Atenda a todas as exigências contidas nesta especificação | **12.1.1** Verifique se A política atende a todas as exigências desta especificação | | | |
| **12.1.2** Inclua um processo anual que identifique ameaças e vulnerabilidades e resulte em um levantamento do risco formal | **12.1.2** Verifique se a política de segurança da informação inclui um processo de levantamento anual do risco que identifique as ameaças e vulnerabilidades, resultando em um levantamento formal do risco | | | |
| **12.1.3** Inclua uma revisão pelo menos uma vez por mês e updates quando houver mudanças no ambiente | **12.1.3** Verifique se a política de segurança da informação é revista pelo menos anualmente e atualizada de acordo com o necessário para refletir as mudanças nos objetivos do negócio ou ambiente de risco | | | |
| **12.2** Desenvolva procedimentos diários de segurança operacional que sejam consistentes com as exigências desta especificação (por exemplo, procedimentos de manutenção da conta do usuário e procedimentos de revisão do registro). | **12.2.a** Examine os procedimentos diários da segurança operacional. Verifique se eles são consistentes com esta especificação e incluem procedimentos administrativos e técnicos para cada uma das exigências | | | |
| **12.3** Desenvolva políticas de uso por funcionários que lidam com | **12.3** Obtenha e examine a política para funcionários que lidam com tecnologias críticas e verifique se a política | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| tecnologias críticas (tais como modems e wireless) para definir o uso apropriado destas tecnologias para todos os funcionários e prestadores de serviços. Certifique-se que estas políticas de uso exijam o seguinte: | contém o seguinte: | | | |
| **12.3.1** Aprovação explícita da administração | **12.3.1** Verifique se as políticas exigem a aprovação explícita da administração para o uso dos dispositivos | | | |
| **12.3.2** Autenticação para o uso da tecnologia | **12.3.2** Verifique se as políticas exigem que todo o uso dos dispositivos seja validado com o nome do usuário e senha ou outro item de autenticação (por exemplo, token) | | | |
| **12.3.3** Uma lista de todos os dispositivos e funcionários com acesso | **12.3.3** Verifique se as políticas exigem uma lista de todos os dispositivos e do pessoal autorizado a usar os dispositivos | | | |
| **12.3.4** Etiquetagem dos dispositivos com indicação do proprietário, informações de contato e objetivo | **12.3.4** Verifique se as políticas exigem que os dispositivos estejam etiquetados com os dados do proprietário, informação de contato e objetivo | | | |
| **12.3.5** Uso aceitável da tecnologia | **12.3.5** Verifique se as políticas exigem usos aceitáveis da tecnologia | | | |
| **12.3.6** Localizações aceitáveis da rede para a tecnologia | **12.3.6** Verifique se as políticas exigem localizações aceitáveis da rede para a tecnologia | | | |
| **12.3.7** Uma lista de produtos aprovados pela empresa | **12.3.7** Verifique se as políticas exigem uma lista dos produtos aprovados pela empresa | | | |
| **12.3.8** Desligamento automático da sessão via modem após um período de inatividade específico | **12.3.8** Verifique se as políticas exigem o desligamento automático da sessão via modem após um período de inatividade específico | | | |
| **12.3.9** Ativação dos modems para os prestadores de serviço apenas quando for necessário, com imediata desativação após o uso | **12.3.9** Verifique se as políticas exigem a ativação dos modems usados por prestadores de serviço apenas quando for necessário, com imediata desativação após o uso | | | |
| **12.3.10** Proibição da armazenagem de dados do portador de cartão nas unidades de disco locais, floppy disks ou outra mídia externa quando os dados do portador de cartão forem acessados remotamente via modem. Proibição das funções de | **12.3.10** Verifique se o uso das políticas exige a proibição da armazenagem de dados do portador de cartão nas unidades de disco locais, floppy disks ou outra mídia externa quando os dados do portador de cartão forem acessados remotamente via modem. Verifique se as políticas proíbem as funções “cut-and-paste” e “print” | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| "cut-and-paste" e "print" durante o acesso remoto | durante o acesso remoto | | | |
| **12.4** Assegure-se de que a política de segurança e procedimentos definam claramente as responsabilidades de segurança da informação para todos os funcionários e prestadores de serviço. | **12.4** Verifique se as responsabilidades de segurança da informação são claramente definidas tanto para os funcionários como para os prestadores de serviço | | | |
| **12.5** Delegue as seguintes responsabilidades de administração de segurança da informação para um indivíduo ou equipe: | **12.5** Verifique a designação formal da responsabilidade de segurança da informação a um Chefe de Segurança ou a outro membro da organização com conhecimentos sobre segurança. Obtenha e examine as informações sobre as políticas e procedimentos de segurança para verificar se as seguintes responsabilidades de segurança da informação foram formalmente e especificamente delegadas: | | | |
| **12.5.1** Estabelecer, documentar e distribuir as políticas e procedimentos de segurança | **12.5.1** Verifique se a responsabilidade pela criação e distribuição das políticas e procedimentos de segurança está formalmente delegada | | | |
| **12.5.2** Acompanhar e analisar os alertas e informações de segurança e distribuí-los ao pessoal apropriado | **12.5.2** Verifique se a responsabilidade pelo acompanhamento e análise dos alertas de segurança e distribuição da informação ao devido pessoal das unidades de administração de segurança e de negócios está formalmente delegada | | | |
| **12.5.3** Estabelecer, documentar e distribuir os procedimentos de resposta a um incidente de segurança e escalonamento para assegurar a administração oportuna e eficiente de todas as situações | **12.5.3** Verifique se a responsabilidade pela criação e distribuição dos procedimentos de escalonamento da resposta aos incidentes de segurança está formalmente delegada | | | |
| **12.5.4** Administrar as contas dos usuários, incluindo adições, exclusões e modificações | **12.5.4** Verifique se a responsabilidade pela administração da conta do usuário e administração da autenticação está formalmente delegada | | | |
| **12.5.5** Acompanhar e controlar todo o acesso aos dados | **12.5.5** Verifique se a responsabilidade pelo acompanhamento e controle de todo o acesso aos dados está formalmente delegada | | | |
| **12.6** Implemente um programa formal de conscientização da | **12.6.a** Verifique a existência de um programa formal de conscientização da segurança para todos os funcionários | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| segurança para fazer com que todos os funcionários estejam cientes da importância da segurança dos dados do portador de cartão: | **12.6.b** Obtenha e examine a documentação e procedimentos do programa de conscientização da segurança e faça o seguinte: | | | |
| **12.6.1** Instrua os funcionários na contratação e pelo menos uma vez por ano (por exemplo, através de posters, cartas, memorandos, reuniões e promoções) | **12.6.1.a** Verifique se o programa de conscientização da segurança provê métodos múltiplos para criar a conscientização e treinamento dos funcionários (por exemplo, posters, cartas, reuniões) | | | |
| | **12.6.1.b** Verifique se os funcionários participam do treinamento de conscientização após a contração e pelo menos uma vez por ano | | | |
| **12.6.2** Exija que os funcionários reconheçam por escrito que leram e entenderam a política e procedimentos de segurança da empresa | **12.6.2** Verifique se o programa de conscientização da segurança exige que os funcionários reconheçam por escrito que leram e entenderam a política e procedimentos de segurança da empresa | | | |
| **12.7** Investigue os candidatos potenciais um cargo na empresa para minimizar o risco de ataques com origem em fontes internas.<br>*Para aqueles funcionários, tais como caixas de lojas, que apenas possuem acesso a um número de conta de cartão de cada vez para executar uma transação, esta exigência é apenas uma recomendação.* | **12.7** Entreviste a administração do Departamento de Recursos Humanos e verifique se é realizado (dentro das limitações das leis locais) o levantamento dos antecedentes dos funcionários potenciais que terão acesso aos dados do portador de cartão ou ao ambiente dos dados do portador de cartão (Exemplos dos levantamentos de antecedentes incluem os empregos anteriores, histórico criminal, de crédito e verificação das referências) | | | |
| **12.8** Se os dados do portador de cartão são compartilhados com o portador de serviço, contratualmente é exigido o seguinte: | **12.8** Se a entidade auditada compartilhar os dados do portador de cartão com outra companhia, obtenha e examine os contratos entre a organização e qualquer terceiro que tenha acesso aos dados do portador de cartão (por exemplo, instalações de armazenagem de tape back-up, prestadores de serviços administrados, tais como companhias de Web hosting, prestadores de serviços de segurança ou aqueles que recebem dados com o objetivo de construir modelos de fraude). Faça o seguinte: | | | |
| **12.8.1** Os prestadores de serviços devem cumprir com as exigências do PCI DSS | **12.8.1** Verifique se o contrato contém cláusulas exigindo o cumprimento das exigências do PCI DSS | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| **12.8.2** Contrato que inclua uma confirmação de que o prestador de serviço é responsável pela segurança dos dados do portador de cartão que possua | **12.8.2** Verifique se o contrato contém cláusulas para o reconhecimento pelo terceiro das suas responsabilidades em relação aos dados do portador de cartão | | | |
| **12.9** Implemente um plano de resposta a um incidente. Esteja preparado para responder imediatamente a uma quebra da segurança do sistema. | **12.9** Obtenha e examine o Plano de Resposta a Incidentes e procedimentos relacionados e faça o seguinte: | | | |
| **12.9.1** Crie um plano de resposta a um incidente para ser implementado no evento do comprometimento do sistema. Assegure-se de que o plano atende, pelo menos, aos procedimentos de resposta específicos, processos de recuperação de negócios e continuidade, processos de back-up dos dados, desempenho e responsabilidades e estratégias de comunicação e contato (por exemplo, informar os Adquirentes e associações de cartões de crédito) | **12.9.1** Verifique se o Plano de Resposta a Incidentes e procedimentos relacionados inclui:<br>• tarefas, responsabilidades e estratégia de comunicação no evento de um comprometimento<br>• cobertura e respostas para todos os componentes críticos do sistema<br>• notificação, no mínimo, às associações dos cartões de crédito e adquirentes<br>• estratégia para a continuidade do negócio após o comprometimento<br>• referência ou inclusão dos procedimentos de resposta ao incidente pelas associações de cartão<br>• análise das exigências legais para reportar os comprometimentos (por exemplo, de acordo com a lei n° 1386 do Estado da Califórnia, é exigida a comunicação aos consumidores afetados no evento de uma suspeita ou ocorrência de comprometimento de qualquer empresa que possua residentes da Califórnia em seu banco de dados) | | | |
| **12.9.2** Teste o plano pelo menos uma vez por ano | **12.9.2** Verifique se o plano é testado pelo menos uma vez por ano | | | |
| **12.9.3** Designe funcionários específicos para estarem disponíveis numa base de 24/7 para responder aos alertas | **12.9.3** Verifique, através de observação e revisão das políticas, de que existe uma resposta de incidente e cobertura de acompanhamento 24/7 para qualquer evidência de atividade não autorizada, alerta críticos IDS, | | | |

| EXIGÊNCIAS DO PCI DSS | PROCEDIMENTOS DE TESTE | INSTALADO | NÃO INSTALADO | DATA ALVO/ COMENTÁRIOS |
|---|---|---|---|---|
| | e/ou relatórios de mudanças não autorizadas em sistemas críticos ou mudanças no conteúdo de arquivos | | | |
| **12.9.4** Forneça o treinamento apropriado dos funcionários em termos das responsabilidades pela resposta a uma quebra de segurança | **12.9.4** Verifique, através de observação e revisão das políticas, que uma equipe responsável por quebras da segurança é periodicamente treinada | | | |
| **12.9.5** Inclua alertas originários da detecção de uma intrusão, prevenção de intrusão e sistemas de acompanhamento da integridade dos arquivos | **12.9.5** Verifique, através de observação e revisão dos processos, que o acompanhamento e a resposta aos alertas dos sistemas de segurança estão incluídos no Plano de Resposta a Incidentes | | | |
| **12.9.6** Crie um processo para modificar e desenvolver o plano de resposta a um incidente de acordo com as lições aprendidas e para incorporar os desenvolvimentos da indústria | **12.9.6** Verifique, através de observação e revisão das políticas, se existe um processo para modificar e escalonar o plano de resposta de acordo com as lições aprendidas e para incorporar os desenvolvimentos da indústria | | | |
| **12.10** Todos os processadores e prestadores de serviço devem manter e implementar as políticas e procedimentos para as entidades conectadas para incluir o seguinte: | **12.10** Verifique, através de observação, revisão das políticas e revisão da documentação de suporte, se há um processo para administrar entidades conectadas fazendo o seguinte: | | | |
| **12.10.1** Mantenha uma lista das entidades conectadas | **12.10.1** Verifique se uma lista das entidades conectadas é mantida | | | |
| **12.10.2** Assegure-se de que são realizadas análises antes da conexão de uma entidade | **12.10.2** Verifique se os procedimentos asseguram que as análises adequadas foram realizadas antes da conexão de uma entidade | | | |
| **12.10.3** Assegure-se de que a entidade cumpre com o PCI DSS | **12.10.3** Verifique se os procedimentos asseguram que a entidade cumpre com o PCI DSS | | | |
| **12.10.4** Conecte e desconecte entidades seguindo um processo estabelecido | **12.10.4** Verifique se a conexão e desconexão das entidades ocorrem seguindo um processo estabelecido | | | |

# Anexo A: Aplicabilidade do PCI DSS para Prestadores de Serviço de Hosting (com Procedimentos de Teste)

## Exigência A.1: Os provedores de serviço de hosting devem proteger o ambiente o ambiente dos dados do portador de cartão

De acordo com o mencionado na Exigência 12.8, todos os prestadores de serviço com acesso aos dados do portador de cartão (incluindo os prestadores de serviço de hosting) devem cumprir com o PCI DSS. Adicionalmente, a Exigência 2.4 declara que os prestadores do serviço de hosting devem proteger o ambiente e os dados de cada entidade à qual prestem o serviço de hosting. Conseqüentemente, os prestadores de serviço de hosting devem levar em consideração o seguinte:

| Exigências | Procedimentos de Teste | Instalado | Não Instalado | Data Alvo/ Comentários |
|---|---|---|---|---|
| **A.1** Proteja o ambiente e os dados hosted de cada entidade (ou seja, estabelecimento, prestador de serviço ou outra entidade), de acordo com A.1.1 a A.1.4:<br>Um prestador de serviço de hosting deve atender a essas exigências, assim como todas as seções do PCI DSS. *Nota: Embora um provedor de hosting possa atender a essas exigências, a compliance da entidade que usa esse provedor de hosting não é garantida. Cada entidade* deve *cumprir com o PCI DSS e validar a compliance de acordo com o aplicável.* | **A.1** Especificamente para a auditoria da PCI do **Prestador de Serviço de Hosting Compartilhado**, para verificar se os **Prestadores de Serviço de Hosting Compartilhado** protegem o ambiente e os dados hosted das entidades (estabelecimentos, prestadores de serviço), selecione uma amostra dos servidores (Microsoft Windows e Unix/Linux) dentro de uma amostra dos estabelecimentos e provedores de serviço hosted e verifique de **A.1.1** a **A.1.4** abaixo. | | | |
| **A.1.1** Assegure-se de que cada entidade tem acesso apenas ao ambiente próprio dos dados do portador de cartão | **A.1.1** Se um provedor de serviço de hosting permite que entidades (por exemplo, estabelecimentos ou provedores de serviço) rodem os seus aplicativos, verifique se os processos desses aplicativos rodam usando um ID único da entidade. Por exemplo:<br>• Nenhuma entidade do sistema pode usar um ID do servidor compartilhado de web | | | |

| Exigências | Procedimentos de Teste | Instalado | Não Instalado | Data Alvo/ Comentários |
|---|---|---|---|---|
| | • Todos os scripts CGI usados por uma entidade devem ser criados e rodar de acordo com o ID único da entidade | | | |
| **A.1.2** Restrinja o acesso e privilégios de cada entidade apenas ao ambiente dos seus próprios | **A.1.2.a** Verifique se o ID do usuário do processo de qualquer aplicativo não é um usuário privilegiado (root/admin). | | | |

| Exigências | Procedimentos de Teste | Instalado | Não Instalado | Data Alvo/ Comentários |
|---|---|---|---|---|
| | **A.1.2.b** Verifique se cada entidade (estabelecimento, prestador de serviço) leu, escreveu ou executou permissões apenas para arquivos e diretórios que possui ou para arquivos de sistema necessários (restritos via permissões de sistema de arquivo, listas de controle de acesso, chroot, jailshell, etc.). IMPORTANTE: Os arquivos de uma entidade não podem ser compartilhados por grupo | | | |
| | **A.1.2.c** Verifique se os usuários de uma entidade não têm acesso por escrito a sistemas binários compartilhados | | | |
| | **A.1.2.d** Verifique se a observação das entradas do registro é restrita à entidade que o possui | | | |
| | **A.1.2.e** Para assegurar que cada entidade não pode monopolizar os recursos de servidor para explorar as vulnerabilidades (erro, raça e recomeçar as condições, resultando em, por exemplo, buffer overflows), verifique se as restrições estão instaladas para o uso destes recursos do sistema:<br>• Espaço de disco<br>• Faixa de freqüência<br>• Memória<br>• CPU | | | |
| **A.1.3** Assegure-se de que os registros de auditoria e de logging se encontram habilitados e são únicos para o ambiente dos dados do portador de cartão de cada entidade e é consistente com a Exigência 10 do PCI DSS | **A.1.3.a** Verifique se o provedor de serviço de hosting compartilhado tem o logging habilitado como a seguir, para o ambiente de cada estabelecimento e provedor de serviço:<br>• Os registros estão habilitados para aplicativos comuns de terceiros<br>• Os registros estão ativos por default<br>• Os registros estão disponíveis para revisão pela entidade que os possui<br>• Os locais onde os registros se encontram são claramente comunicados à entidade que os possui | | | |
| **A.1.4** Habilite os processos para que possa haver investigação rápida no caso de um comprometimento em qualquer estabelecimento ou provedor de serviços hosted. | **A.1.4** Verifique se o provedor compartilhado de hosting escreveu políticas para que possa haver investigação rápida dos servidores relacionados, no caso de um comprometimento. | | | |

# Anexo B – Controles Compensatórios

## Controles Compensatórios – Geral

Os controles compensatórios podem ser considerados para a maioria das exigências do PCI DSS quando uma entidade não pode atender a uma especificação técnica de uma exigência, mas tenha diminuído suficientemente o risco associado. Consulte o Glossário do PCI DSS para a definição completa dos controles compensatórios.

A efetividade de um controle compensatório depende das particularidades do ambiente no qual o controle é implementado, dos controles de segurança à sua volta e da configuração do controle. As empresas devem estar atentas para o fato de que um controle compensatório em particular não será efetivo em todos os ambientes. Cada controle compensatório deve ser completamente avaliado depois da implementação, para assegurar a efetividade. A orientação a seguir provê controles compensatórios quando companhias não puderem tornar os dados do portador de cartão ilegíveis de acordo com ar exigência 3.4.

## Controles Compensatórios para a Exigência 3.4

Para companhias que não forem capazes de tornar os dados do portador de cartão ilegíveis (por exemplo, através de criptografia) devido a limitações técnicas ou do negócio, os controles compensatórios podem ser considerados. *Apenas as companhias que empreenderam uma análise de risco e possuem limitações tecnológicas ou limitações empresarias documentadas e legítimas podem considerar o uso de dos controles compensatórios para atender à compliance*.

As empresas que considerem os controles compensatórios para tornar os dados do portador de cartão ilegíveis devem compreender o risco aos dados imposto pela manutenção dos dados legíveis do portador de cartão. Geralmente, os controles devem fornecer proteção adicional para a diminuição do risco imposto pela manutenção dos dados legíveis do portador de cartão. Os controles considerados devem ser em adição aos controles exigidos no PCI DSS e devem satisfazer a definição de “Controles Compensatórios” do Glossário do PCI DSS. Os controles compensatórios podem consistir tanto de um dispositivo como uma combinação de dispositivos, aplicativos e controles que atendam a **todas** as seguintes condições:

1. Prover adicional segmentação/abstração (por exemplo, na network-layer)
2. Prover a habilidade de restringir o acesso aos dados do portador de cartão ou aos bancos de dados com base nos critérios a seguir:
    - Endereço de IP / endereço Mac
    - Aplicativo / serviço
    - Contas do usuário / de grupos

- Tipo de dados (filtragem de pacote ou packet filtering)

3. Restringir o acesso lógico ao banco de dados
    - Controle do acesso lógico ao banco de dados independentes do Diretório Ativo ou Lightweight Directory Access Protocol (LDAP)
4. Prevenir/detectar aplicativos comuns ou ataques ao banco de dados (por exemplo, SQL injection).

# Anexo C: Planilha/Exemplo Preenchido dos Controles Compensatórios

## Exemplo

1. Limitações: Enumere as limitações que impedem o atendimento da exigência original

   A Companhia XYZ contrata os Servidores Unix com LDAP. Dessa forma, cada um deles exige um 'root' login. É impossível para a Companhia XYZ administrar o 'root' login e também é impraticável registrar todas as atividades 'root' para cada usuário.

2. Objetivo: Defina os objetivos do controle original; identifique o objetivo atingido pelo controle compensatório

   O objetivo da exigência de logins únicos é duplo. Primeiro, não é considerado aceitável a partir de uma perspectiva de segurança para o compartilhamento das credenciais do login. Segundo, os logins compartilhados tornam impossível determinar definitivamente se uma pessoa é responsável por uma ação em particular.

3. Risco Identificado: Identifique qualquer risco adicional implicado pela falta de controle original

   O risco adicional é introduzido ao sistema de controle de acesso quando não é possível assegurar um ID único a todos os usuários e não é capaz de ser acompanhado.

4. Definição de Controles Compensatórios: Defina os controles compensatórios e explique como eles atendem aos objetivos do controle original e o aumento do risco, se houver algum.

   A Companhia XYZ vai exigir que todos os usuários façam o log nos servidores dos seus computadores usando apenas o comando SU. O comando SU permite que o usuário acesse a conta 'root' e execute ações dentro da conta 'root' mas que não seja capaz de fazer o log in no seu diretório su-log. Dessa forma, cada uma das ações do usuário pode ser acompanhada através da conta SU.